Welcome

maandag 26 september 2016 06:39

Welcome everyone, I will use this OneNote to share my notes with you for the sessions that I will attend.

I hope you enjoy this and please leave a comment on my blog if you have any questions

https://www.arjancornelissen.nl/2016/09/26/ignite-2016-atlanta/

KeyNote

maandag 26 september 2016 06:32

Julia White starts the keynote with a recap of what happened since the last 18 months
This is the largest IT conference in the world.
IT changes fast even Julia had trouble keeping up with the changes when she changed her job within Microsoft
You need a grow mindset to keep up.
Satya will do his keynote later today.

Scot Guthrie
It is about digital transformation.

- Engage customers like BMW did with there in car systems. They did this from concept to production in under a year. Facebook did this also with Office 365.
- Adobe is using Azure as cloud platform and uses that for their SaaS solutions

Satya talks to Adobe how they uses Azure

- They use it for their document cloud, creative cloud and marketing cloud
- Adobe changed their whole company to be cloud first
- The next face of innovation for Adobe was to enable all customers a cloud first experience.
- And digital transformation with document creation
- There will be an integration with Adobe and Dynamics 365, this will create an integrated marketing platform
- Also an integration with PowerBi and PowerApps will be coming

IT transformations

- Customers are going cloud first and need to adopt new technologies, it will be a great and fun era
- With using the cloud IT pro's are getting time to innovate instead of keeping everything to work.
- Be open to the cloud, but now what you are doing is important

Cloud

- The move to the cloud is a journey that will help building better productivity, business apps, create application innovations, Data & intelligence.
- Microsoft Cloud is the only cloud that provides the depth and breath.
- Now 34 Azure regions, that is twice that AWS has.
- The Azure cloud is certified with over 30 certificates
- It is the only cloud that can work out of China and Germany
- It had unique hybrid capabilities with Identity, infrastructure, data and business apps
- >85% of Fortune 500 are using the Microsoft Cloud

- Azure is the foundation of all cloud services that Microsoft is offering
- It has choice and flexibility with a lot of applications and operating systems
- Hybrid management and security
- Demo of new features:
    - New preview of Azure Monitor, that will monitor all your machines on-premises or cloud. VMWare or Microsoft.
    - You can have charts and alerts to every machine and resources. It uses SCOM agents and with the logs search you can search all logs from every machine in the monitoring
        - Search uses the SQL query form
    - This is part of the OMS suite.
    - Overview of updates and what machine has what updates.
    - Create your own dashboards

Security center gives the health of your machines and infrastructure. It gives recommendations on the possible breaches

Azure stack 2 preview is announced today
Windows Server 2016 is cloud ready, Azure inspired, built-in Docker containers, Nano deployment.
All windows server 2016 get the commercial Docker implementation at no extra cost.
It is now GA. This is also for System center 2016

App modernization + DevOps
Xamarin is included in Visual Studio.
Xamarin test cloud makes it possible to test your applications on physical devices.
Visual Studio Team Services provides a complete DevOps solution.
It also contains release management, with extra tests, approvers.
No matter what language or platform you use, you can use Visual Studio Team Services
It has complete integration with all Azure products

More personal computing
The vision of Microsoft what comes
Computing will get more personal and intuitive.
In 2020, 43% of the US workforce will be freelances
In 2020 there will be 44 zettabytes of data in storage.

Secure Productive Enterprise
Windows 10
Three releases since the launch, 400 million active devices
Department of Defense is using 4 million devices
Office 365
70 million active users every moth
EMS (Enterprise Mobility + Security)
SSO and MFA for SaaS apps,
Azure Active directory has 1 billion logins every day

New features
Windows 10 deployment in the enterprise
Ink can convert ink to digital data like your flight data or stock information.
Ik can be used in Office to strike out text in documents, also highlights in a document
Ink in One note can solve math when you select a formula
It does not only work with Microsoft products, but also with Adobe Illustrator or you own product with only a few lines of code
In a Word document you can keep track of the changes when collaborating with multiple coworkers
In Outlook you can use Delve Analytics what the activity is on the email that you have send out
Delve Analytics is like the Fitbit of work. Not only analytics with meetings and coworkers, but also with customers.
The Microsoft Hub is one of the best devices to use in a meeting to get it started in a few seconds instead of minutes.
No more photos of the whiteboard, it is al saved and mailed.
When done, everything is removed and set back to public use.

Security is a never ending battle, the endpoint are always at risk.
According the FBI there are 2 types of companies, the one that know that they are hacked and the ones that does not know.

Intelligent Security Graph makes it possible to get intelligence where the breaches comes from and what attacks there are.

Announcement

Windows Defender Application Guard, this is for Microsoft Edge and hardware based.

This will be available to The Windows Insiders.

The passwords are protected with Windows Defender Application Guard.

No matter how good your guard is you will be attacked.

Office 365 and the Windows Defender work together to block further distribution of infected attachments

Secure and manage your digital transformation

maandag 26 september 2016 11:11

GS06
Brad Anderson

Going further where the Keynote left off

Cybersecurity te the #1 priority, the attacks are more advanced and more damaging
Data is more and more on devices and in the cloud and we need to secure it. The perimeter as we knew is not there anymore. We are used to build guards around the perimeter.

Old defenses are not sufficient for the new attacks, we need to defend ourselves for that.

Microsoft build the Microsoft Intelligent Security Graph for this.
Every day this graph learns from all the Azure AD logins, emails send, Bing searches and attacks on Azure, Xbox and all other services that Microsoft runs.

With this kind and amount of data they can use this to defend better

Microsoft spends 30 billion on security R&D

Security has to be built in and engineered so that the user does not know that it is there.

The security posture
- Protect
- Detect
- Respond

Protect:

Define the rules as and IT pro that secures the gates
Identity it the new control plane, this is the new perimeter.
The root cause of >75$ of intrusions are compromised credentials.
In private preview, access protection on apps on mobile devices
Logins with SaaS apps in Azure AD feeds the Microsoft Intelligent Security Graph
When using MFA you do not want the user to ask for it every time
Azure AD Identity protection center (EMS license)
    Put policies in place based on identity risks
Privilege identity (Just in time) (EMS License) is also new
EMS console in Azure portal, very useful when using Azure AD Premium and Intune.
    Policies can be built on
        App risk
        Location risk
        Identity risk

Detect

58% of the people have accidentally sent data to the wrong person.
The design principals are there for the people with the right intend
Only protect the company data and not the personal data on a device, the Office applications has this option
Not only Microsoft Apps have these capabilities, apps like SAP, Adobe have this. As a vender you can built this into your own app. This is available on all three mobile platforms
Data should be self-protecting. The document should know who can access it.

Microsoft bought a company that has the capabilities to classify documents. When an employee forgets it, this tool can do this automatically with rules.
With this You are in control of your data
New in EMS, Cloud app security, this came from the most recent company that Microsoft bought.
This is an amazing tool for the security offices in your company
Security center is free to use for everyone and available in Azure portal

Respond

Always assume breach
The Microsoft Operation Management Suite can be used to respond to breaches. OMS is built by the Operational management team. It can control services that are in Amazon, Azure, your own datacenter.
Security and audit can give insight where machines or service is accessed from.
Attacks can be very simple, just by a macro in a Word document that is attached in an email.
The Windows Security Center has an amazing drill thru on breaches and where it came from, what happened during the breach. This has great power in securing your environment.
Together with EMS you can respond with confidence.
The power of the cloud helps with your protection.

Config manager is now updated every month. Config manager is used for the majority of the Windows 10 upgrades.
Windows Hello is a dual authentication, because you need your device and your face.

Secure Productive Enterprise

Windows 10
Office 365
Enterprise mobility + Security

Discover what's new and what's coming for Office Delve

maandag 26 september 2016 14:05

BRK2044
Cem Aykan (Senior Program Manager)
Mark Kashman (Senior Product Manager)

There is a separate session for Delve Analytics. It is renamed to MyAnalytics.
Office Delve is majorly part of the intelligence, but has parts in Collaboration, Mobility and Trust.
It is really reinventing productivity

Delve is in a few words a discovery service that will discover relevant content & people.
Search is when you know a part of what you are looking for, discovery is when you do not know what you are looking for, but gives you what relevant is for you.

The Microsoft Graph is the base of Office Delve. It gets all the info from SharePoint, OneDrive, Outlook and other Office 365 apps.

The new SharePoint tile uses the Graph to display content and suggested sites based on Delve.

In OneDrive for business you have a discover button that will show all suggested files that might be relevant for you. This will also come to the mobile app. It will not show sites, only document, even documents that are not on OneDrive

In Delve you can also create your own boards with search words (tags)
When you search from delve, it gives you back the most relevant content for you.

You can also go to someone's profile to look what documents that person shared with me.

How can you control delve?

- In the feature settings, you can as a user opt-out of Delve, this can be done for documents and analytics
- The admin can do this also for everyone

Delve does not change any permissions
It is search in the basics and is security trimmed.

Evolving "People experiences" throughout Office 365

- Delve Windows 10 APP
- Intelligent People Cards
- Office 365 Profile

The app works with MFA authentication. On the people part you see the number of updates that the persons around you. It is a universal app, so works on mobile and pc.
The me part of Delve is a great way to get back to work on the documents you were working on earlier. Before this the profile was just a place where you came once.

Intelligent people cards works in Outlook, it is the hover card that we already know. This gets information from Delve. In Outlook Online, this has more options and showed as a side pane like an app.
The people card in SharePoint and OneDrive is changed a lot and way better. It is an involvement from the Skype 4 Business status bubble.
The document scope here is by default to the library, but you can change this scope
You cannot customize the info on the card for now. These cards get more advanced in the coming time

The profile update is changed also, it looks more on the SharePoint Profile.
It will become an enterprise profile

The "platform" section

- Delve Hybrid
  - You need hybrid search and use Office 365 profile. With hybrid search only the index is in the cloud, not the content itself.
  - You need to be in a form of hybrid to have Delve. It will not be available as a complete on-premises product.

Great blog post
https://blogs.office.com/2016/09/26/create-better-work-habits-with-myanalytics-formerly-delve-analytics/

The Office 365 profile is expanded and has the same properties as the SharePoint profile. It is best to use and expand the Office 365 profile instead of the SharePoint profile. The updates from the Office 365 profile pushes updated to the SharePoint profile.

Innovation session

maandag 26 september 2016 16:03

Satya
Microsoft Mission:
Empower every person and every organization on the planet to archive more

In 2015 we created 1 zettabyte of data. We are getting to a point that we do not know how to name documents

Microsoft is democratizing AI
For every person in every organization.
They will do this in 4 applications

- Agent (Cortana) It knows you, your context, your work and it knows the world
  - 133 million active users around the world, 12 billion questions
  - Cortana is also responsible for the notifications on your windows PC
  - Integration with Wunderlist and sticky notes
- Applications
  - Office 365 and Dynamics 365, knows your work and your organization
  - Word has a better grammar and spell correction due to the understanding that Microsoft has about how people write
  - MyAnalytics, Office analytics new name
- Services
  - Cortana intelligence
  - Machine learning & Advanced intelligence
  - Bot framework
  - Sport and election predictions
  - Cognitive Service API
  - Uber uses image recognition to do real time identity verification
- Infrastructure
  - Azure
  - Hyper scale can translate all English words on Wikipedia in 0,1 seconds; it takes a human 0,2 seconds to blink; Bing searches uses this already

Accelerate your Office 365 deployment with FastTrack

dinsdag 27 september 2016 08:51

BRK3065
Scott Miller (FastTrack Principal Group Program Manager)

FastTrack migrates, Email, Contacts, Calendar, OneDrive, Google Drive, Box, file shares

The FastTrack team keeps learning, this session is about what they learned with interacting with the customers

FastTrack is Onboarding and adoption assistance
It is included for all customers above 50 seats
Exchange, SharePoint, Skype, Yammer and Office including E5 support
EMS - Intune and Azure AD Premium Enablement
Service onboarding and user adoption assistance
Email migration and file migration

If you are not yet using it, get in contact with the FastTrack system (http://fasttrack.microsoft.com)

They start with the planning, help moving and boost user engagement

FastTrack supports 12 languages and support the whole world

Facts

- 600+ engineers
- 51K+ success plans
- 4K+ new customers in FastTrack per month
- 22K+ Customers enabled
- 2.45 PB of data migrated
- 3.3M seats migrated
- 185 Customer Satisfaction (NSAT) (Max score is 200, the goal is 190)
- You can run thru the FastTrack multiple time for different products

The process

- Identify the key stakeholders
  - Why do you want to move to the cloud
- Define the vision and business scenarios
  - What is the vision of the goals, what scenarios are there to make it successful
- Plan for a successful rollout
  - What metrics do the company have their self

They have a few scenarios where to start from.
The FastTrack team helps determine what services you should deploy to make the scenario successful

- This is part of the envision session

When the envision sessions are done, the technical onboarding is started with preparing the infrastructure and ensure that the migration is smooth.
The team only helps you with the steps (guidance), they do not fix the issues.
Decide if you need to move the data or not. If you move the data you move the users

You have ongoing access to FastTrack engineers, guidance on AD, Network, DNS, tenant and user setup

Deployment architecture and guidance , adoption planning workshop, templates and guidance for end user communication and persona-based productivity scenarios.

You as customer with or without your partner needs to do the work.
See the deck for the responsibilities

EMS FastTrack session on Thursday at 9:00

Exchange Onboarding
- Core onboarding and adoption planning.
- When you have 20K+ seats there are a few more benefits like, Exchange Unified Messaging guidance, public folder coexistence

SharePoint Onboarding
- Core onboarding and adoption planning

Skype for Business
- Core onboarding and adoption planning
- Provisioning
- PSTN

They try to drive value
- Boost user engagement and drive adoption
- Manage and prepare for change
- Measure success, learn and iterate

Use training, video's and sessions to drive value

Formula for adoption
- Begin with the requirements + Accelerate with success factors

- Requirements
  - Due date
  - Intent
  - Business reason
  - Success Owner
- Success factors
  - Stakeholders
  - Scenarios
  - Awareness
  - Training

The FastTrack team will help to define these 8 things

The FastTrack wizard is context aware, questions are only asked when necessary and dynamic

Slides are on Channel9

Get updates to Remote Desktop Services in Windows Server 2016 an Azure

dinsdag 27 september 2016 09:49

THR2140
Scott Manchester (Principal Group Program Manager)

RDS is optimized for cloud deployments, graphics (GPU virtualization)
A GPU can be mapped to a VM, the VM has the bare metal drivers to have the best performance.
The GPU mapping is ideal remote 3D and rendering of large and GPU intensive workload
Demo was done on a Azure N-SKU VM. These are now in preview and will be GA later this year
http://gpu.azure.com to sign up for the preview

You can even play games when you have a GPU mapped to a VM
This is called: Discrete device assignment.

The connection broker is also updated to manage the big amount of connections at a single time
With RDS10 the connection times are improved a lot

RDS on Azure can use templates, there are over 400 templates, if you search for RDS you will find 4
Azure.microsoft.com and search for templates under documentation

Manage Microsoft Office 365 Groups

dinsdag 27 september 2016 14:09

Eric Zenz (Principal Program Manager Lead Office 365 Groups) @ericzenz
Vince Smith (Senior Program Manager Microsoft Identity Services)

Office 365: Complete Group collaboration solution
Addressing the unique needs and workstyle of each group

It is one group system across Office 365

- It is one identity in Azure AD, everyone in that group has access to the resources
- At creating a group, a Group is created in AAD, a mailbox is created, a site in SharePoint is created, local group if applicable.

Groups can be administered in the UI and thru PowerShell

- Office 365 Admin center
- Office 365 Admin app
- Azure AD Admin Portal
- Exchange Admin console
- *-UnifiedGroup / *-MsolGroup
- *-UnifiedGroupLinks (Membership updates)
- *-MsolSettings (setting tenant policy of individual policy)

If you use distribution groups, consider to migrate to Office 365 Groups (Unified Groups)

Directory Management,

- Naming policy
  - New: the naming policy doesn't apply to DLs synched from on-prem
  - IT admins can override
  - Creating a group from planner does not use this naming convention for now
  - Block word, list, pre-/post-fix based on AAD attributes
  - **Will be replaced by AD policy in Fall 2016**
- Group creation permissions
  - AD policy can restrict some users from creating groups anywhere in Office 365
  - Does not prevent users from using groups
  - IT can still create groups
- Dynamic memberships
  - Need AD premium

Group Policies

- Usage guidelines
- Data classification
- Hidden membership
  - Native PowerShell is coming, for now only the graph API beta endpoint works for now.
  - See slides for the command

In the new Azure portal the groups are exposed as type "Office"
Dynamic membership rules syntax looks like PowerShell syntax where clause

Get-MsolAllSettingTemplate can be used to get a Unified Groups template to start with.

Use this to create a pilot group that is able to use groups.

Directory Management - what's next
Expiry and soft-delete

Admins set a policy
The group owner gets an email
Group owner renews group
Soft delete option, 30 days after deleting it is able to restore, this includes email, notes, tasks, files and membership

Profanity checking and banned words
A list of profanity words provided by Microsoft and custom word block list. The list from Microsoft is available in 100+ languages

Naming policy
No matter where a group is created, strings or user properties can be appended to the group name.

Extensibility / Programmability
Using the Microsoft Graph
Start with the Microsoft Graph Explorer at https://graph.microsoft.com
https://graph.microsoft.com/v1.0/groups
https://graph.microsoft.com/beta/groups
The Microsoft Graph is a RestFull interface
/groups/<ID>/Conversations get all conversations in that group
/groups/<ID>/Setting you are able to add a setting to a group like setting a policy

Use the Microsoft Graph for all new apps, The AAD graph will stay for existing apps.

Security, Compliance, Audit
Mobile application management for groups, now iOS and Android
Privacy conversion is now available, you can change the privacy of the group

Guest access to Office 365 groups.
Tenant wide -> no guest can be invited to any of the services
Guests in Groups -> can be found under Services & Add-Ins -> Office 365 groups.
Invite guests to a specific group, this can only be done with PowerShell
Specific group -> with PowerShell

eDiscovery is supported for groups, when you do that, you need to do a search on both Exchange and SharePoint
Preservation and deletion is available.
Auditing can be done thru
Azure AD admin portal
Audit log search in Office 365 admin center
PowerShell: Get-UnifiedGroup

Reports
Group usage in the portal
File quota management can be done with Set-SPOSite in PowerShell

Migrating Distribution lists to Groups
Eligible:
Create in the cloud
Not nested
No join or depart restrictions
Not dynamic membership
No delivery status notifications configured
No contact
Not hidden from address list
Public folder to Office 365 Groups can be done with third party tooling

In hybrid
Cloud mailbox users have a full integrations
On-prem mailbox see it as a Distribution list if
Group writeback

Need SPO license

Need an Exchange hybrid configuration

Group survey

http://aka.ms/groupsurvey

Metalogix meeting

woensdag 28 september 2016 09:00

Had a demo about the metalogix tooling at their boot.
They explained what their tooling can and what capabilities would be great for my customer.
They have an option to import SKOS files for Managed Metadata, It seems that this is an open standard. I never heard about it.

Engage and inspire your organization with videos using Microsoft Stream & Office 365 Video

woensdag 28 september 2016 08:58

BRK2237
Nagu Rangan (Product Marketing Manager - Azure)
Marc Mroz (Program Manager - Azure Media Services)

Organizations need a better way to manage, share and communicate with video internally and externally with partners and customers.
Office 365 Video is a video solution that is available only for Office 365 subscribers
Microsoft Stream is a video solution for all businesses, not only the ones with an Office 365 subscription

Both products are own and build by the same team
In time the products will merge into one product with no effort on the customers side.
When you are an Office 365 customer you can keep using Office 365 Video

Permissions on Microsoft Stream is on the file level, for Office 365 Video this is on channel level. When merged both are possible.
In 28 days they have 1M active users, 7M uploads, 4.5 M activated users.

More and more organizations are using video to train and share data. Mark and Spencer and Adidas are great examples of this

In Stream you can add a video to multiple channels, this is not possible in Office 365 Video.

All videos are distributed by CDN and are there in chunks. These chunks are encrypted so nobody can watch it without login.

Integration can be done with Sway for both Microsoft Stream and Office 365 Video
Embedding a video is like the YouTube. On the new SharePoint pages it even resizes.
OneNote knows it is a video if you past the embedding video

Microsoft Stream does not need SharePoint, is uses Azure for the storage and for the metadata.

The video's will never use more streams then the original bandwidth is.
Videos are playable directly.

What's new in Office 365 Video
Better metadata updating
Better integration with Office 365 Video in the SharePoint tile in the waffle
External authenticated sharing is coming, now under development
1080P is coming
Access for Kiosk Users is coming in view only

Vision and roadmap
My Hub
- Creating one portal for all video content
- Get embed codes, sharing video

Search & Discovery
Live streaming in portal
- Integrating with Skype meeting broadcast

Analytics & Intelligence

- Deep search, transcoding audio, faces, emotions, OCR

Ecosystem

- API access
- Integration with PowerApps and Dynamics
- Partner offerings for content creation and distribution

Media Intelligence

Transcoding a video, recognition of the people in there and even when in the video they are talking

Simple tools for creating video

- Skype for Business
- PowerPoint Mix
- A lot of 3rd party tools

Creative video ideas

- "On the way to lunch" interviewing someone with a dashcam
- Virtual staff meetings
- New product info

Network traffic optimization & Caching

- Microsoft is partnering with 3rd party for caching from the CDN; Videos are in Unicast so every user downloads the video
  - Ramp (Works today)
  - Hive (finishing integration in O365 video and beta testing)
  - Kollective (under development, to be integrated into Office 365 Video)

Statistics on the videos are available

Learn best practices for Customizing and Branding SharePoint Team Sites

woensdag 28 september 2016 10:36

Tejas Mehta (Senior Program Manager SharePoint Experience Team) @tpmehta
Eric Overfield (Office Servers and Services MVP) @ericoverfield

This session is about branding the existing team sites, not the new ones

- Best practices
  - Have a plan
    - Know the purpose(s) of your sites
    - Have clear governance - self services, guest, information protections
  - Optimize for team collaboration
    - Leverage library functions
    - Encourage file sync
    - Enable external collaboration
  - Standardize & reuse
    - Make use enterprise vocabulary & taxonomy
    - Define templates
- UI/UX
  - Team sites must convey purpose
  - No content overload
  - It is about the content, keep branding low
    - Office 365 Theming
    - Composed Looks
    - Alternative CSS
    - JavaScript Embed
    - Custom masterpage
      - It is supported for classic team sites and will be for the foreseeable future

The classic teamsites will be depricated, but this will take some time, there is no timeframe for this. The SharePoint framework needs to be ready for this and the metrics need to show that the SharePoint framework is widely used

- Start your branding with Office 365 themes and SharePoint themes
  - Office 365 Theme is global and your users are able to update this if the tenant admin allows this
  - SharePoint Theme tool: SharePoint Color Palette Tool; this tool let you create a color file
    - Remote deploying the SharePoint theming with Office Dev PnP; adding the files can be done with provisioning template with only those files to provision

      For now the composed look will not work well with a team site in an Office 365 group
  - Alternative CSS
    - This cannot be used with the SharePoint Framework
    - Can be set thru the browser if publishing is enabled, use CSOM API by setting the AlternateCSSUrl

      Learn modern toolchains
      - NodeJS, Yeoman, Gulp, SASS, etc
  - JavaScript Embed
    - Add reference to custom JavaScript without a custom master page
    - Never update the ribbon with this
    - If Microsoft changes the ID's, you need to update your JavaScript
    - You can use a tenant wide CDN (just announced) or for development NodeJS

- Custom masterpage
    - Do this only if you have really good reasons, the JavaScript Embed has a lot of options that is for most customizations enough
    - Using a custom masterpage is sort of forking of the version you start with. You do not get the new features that Microsoft releases.

All code can be found on Github, links are in the slides
Never set your production environment to first release, do it for a few users and not for the whole tenant.

Collaborate outside the firewall with Office 365 Groups

woensdag 28 september 2016 12:45

BKR3250
Shashi Singaraval (Principal Program Manager)

How and what can I share

- You can add external users just like adding an internal user, only type the complete email address
- When this is done, there is a globe behind the group name and when sending an email you get a mail tip
- A guest cannot be changed from member to owner
- A guest get emails, calendar invites and can collaborate on the files and the OneNote
- It works with both organization and personal accounts
- When an external user get an invite email, he/she can leave the group. When he/she decides that they want to be part of the group again, that is possible when clicking on the link in the you have left email. The owner of the group has to approve this request.
- Only the owner of the group can add guests and approve guests

- Planner integration is coming
- This is available now on the web, mobile and desktop is coming this year

Architecture

- It is a single identity in Azure AD and synced to Exchange and SharePoint.
- Azure B2B is supported.

What admin controls and how to manage external users

- You can set guidelines for the external users, by default it redirect to Microsoft
- Adding a guest can be controlled at three levels; See Manage Microsoft Office 365 Groups
  - Organization level
  - For all groups
  - For a specific group

Reporting and Auditing

- This can be done thru the Office 365 usage reports and Azure AD Portal
- Also with PowerShell using the Get-UnifiedGroupLinks cmdlet
- All settings are done in Azure AD so every application is aware of this

Guest cannot access IRM messages

Throw away your DMZ - Azure Active Directory Application Proxy deep-dive

woensdag 28 september 2016 14:07

BRK3139
John Craddock (Identity and Security architect at XTSeminars) @john_craddock

DMZ Challenges?

- Hardware costs
- Maintaining security
- Authenticating users at the edge
- Authenticating users to webservers in the DMZ
- Maintaining VPN for remote workers

Azure AD Proxy is a service that exposes an public IP.
On-premises you need a machine that creates the connection and only outbound firewall rules.
You can have multiple connector machines for performance.

The new portal for Azure AD is in public preview since the 22th of September

Prerequisites for the Azure AD Application Proxy

- Requires Azure AD basic or premium (p1 or P2) subscription
  - https://www.microsoft.com/en-us/cloud-platform/azure-active-directory-features
- Connector must be installed on
  - Windows Server 2012 R2 or higher (be careful now with Windows Server 2016)
  - Windows 8.1 or higher
- The on-premises firewall must be enabled for outbound traffic from the connector
  - http://test.cloudapp.net for testing the ports
- Download the connector from the Azure Portal when you enable the Application Proxy
  - A troubleshooter is included

Ports

- 80
- 443
- 10100 - 10120
- 9352,5671
- 9350
- 8080
- 9090
- 9091

Publication of the applications is only available in the classic portal
You need to specify an unique name, the internal URL of the application and the pre authentication method

All users must have the license and be assigned to the application

The default external URL will be "https://<name>-<tenantname>.msappproxy.net"
You can add a custom domain, that must be in Azure AD and have a own certificate

When you do not enable pre authentication you are pass thru the proxy to your application as an anonymous user.
With pre authentication on Azure Ad your application still see you as anonymous

Authentication to Applications

- Anonymous
- Forms
- Kerberos with KCD
- NTLM -> DO NOT USE THIS unless nothing else works
- Token authentications

The machine that runs the connector must be domain joined
In Azure AD you have the option to select the Delegated Login Identity

- User principal name
- On-premises user principal name
- Username part of user principal name
- Username part of on-premises user principal name
- On-premises SAM account name

Before you start check if the application can be used with kerberos
When you use Kerberos, in Azure AD you need to set the SPN

Claims aware applications need to authenticate itself to an STS.

- To use OpenId you need ADFS on server 2016

When your application has a different authentication broker you get 2 logins, so no SSO
If your application trusts Azure AD you get SSO or if the user is an federated user the same ADFS users is used.

Microsoft has partnered with PingAccess, this is coming to Azure AD

Troubleshooting whitepaper
http://aka.ms/proxytshootpaper

Learn about PnP and the new SharePoint Framework

donderdag 29 september 2016 08:48

BRK2115
Vesa Juvonen

Office Dev PnP teams goal was to create a community that will share their knowledge and that you do not have to bang your head on all the search engines to find the correct answers
The team is not officially part of the Patterns and Practices team of Microsoft.

More than 2000 tenants user PnP Core component
More than 1 billion requests using PnP Core Component during the past 3 months
Over 150 samples available
PnP is now owned by the engineering team

The URL to start: http://aka.ms/SharePointPnP

The code from Office Dev PnP is validated by the product team.

Anything in PnP initiative is FREE TO USE

Every Monday there is a blog post on http://dev.office.com/blogs
    Here you can find all webcasts, communications and monthly overview
All samples can be found on dev.office.com, you do not need to go to GitHub for this.

All videos and webcasts can be found on http://aka.ms/SPPnP-Videos
All documents: http://aka.ms/SPPnP-Docs, even this presentation
    All slides with the technology explained can be found there and can be reused

What is in there to use in production
    PnP .NET Core
    PnP PowerShell; does not compete with the admin PowerShell cmdlets
    PnP Partner Pack; is a starter kit with the most common used components; https://github.com/officedev/pnp-partner-pack
    PnP JS Core; this is started because of the SharePoint Framework; it can be used for both the SharePoint framework as the current SharePoint solutions
    All kind of components and solutions

The core CSOM is extended with new functions, if you have an reference to the core CSOM and have a reference in your project.

Execute-SPOQuery does the same as $ctx.ExecuteQuery()

The Partner pack has also an option to create an template from existing sites, an overview of the sites from me; refresh sites with the template

PnP JS Core can be used in TypeScript
You need to do a pnp.setup() once for the connection to your tenant
It uses promises in JavaScript
Can run on NodeJS

The SharePoint Framework and future models
    The framework is in dev/preview now, it will be released in preview tenant soon

Documentation, tutorials, samples and videos: http://dev.office.com/sharepoint
Update to documentation and samples are very welcome
GitHub: http://github.com/sharepoint

Get started with this, it will take 1 hour to setup your environment and about 2 hours to go thru the getting started tutorial
The tutorials are also available on YouTube

Access SharePoint files and lists using SharePoint API in Microsoft Graph API

donderdag 29 september 2016 10:36

BRK4016
Luca Bandinelli (Prinipal Program Manager)
Ryan Gregg (Principal Program Manager)

What is Microsoft Graph?
- The one API to get them all
  - /me
  - /users
  - /groups
  - /messages
  - /drive
  - And more
- Accessing insights /insights/trending
- Traversing data /drive/items/<id>/lastmodifiedByYser
- Works with both work and personal accounts

Announcing: SharePoint in Microsoft Graph API
- It is an early beta
- Give feedback what needs to be added
- Shows the direction for the feature

The namespace for the Graph is /sharepoint; it is only available on the beta endpoint
Getting the sites /beta/sharepoint/sites
Getting a specific site: /beta/sharepoint:/sites/facilities to get the site https://<tenant>sharepoint.com/sites/facilities
There is a bug now that you need to replace the names with the guids to get it to work

For now
- Find SharePoint artifacts (sites/lists/ list items
- Add, update and delete items

It follows the new Microsoft REST API Guidelines

Usage scenarios
- /drive entity
  - Access to files
  - Best if your application is files focused
- /list entity
  - Access to all list item entities
  - Best if your application is SharePoint focused
  - Access to custom columns, data types and other SharePoint concepts

Files are available thru both endpoints

For now only the default fields that are indexed you can sort on.

You can switch from the Microsoft Graph to the REST API without reauthenticating

They are working on support of OpenID in SharePoint

Two great demo's how to use the graph API to get data into SharePoint from a IoT device and the new SharePoint Framework to show it.

SharePoint REST/CSOM isn't going away

Resources

- https://Graph.microsoft.io
- https://Github.com/sharepoint
- https://Github.com/onedrive
- https://Officespdev.uservoice.com
- https://Github.com/MicrosoftGraph

Deploy and provision best practices with Microsoft SharePoint Server 2016

donderdag 29 september 2016 12:25

BRK3035
Jason Himmelstein @sharepointlhorn
Todd Klindt @toddklindt

Infrastructure design
- Analyze customer requirements
  - High availability -> what does it mean for the customer
  - Disaster recovery -> what are the RPO and RTO
  - Budget constraints -> the number of 9s that you can reach
  - Location awareness -> internet speed, location of the customer and the datacenter
  - Number of concurrent users -> the size of the farm, how many users now and in the feature; what is the plan for hybrid?

2013 Basic Topology
- Web server(s)
- App server(s)
- Database server(s)

  2016 topology is not the same, so start from scratch

2016 basic topology
- Web server(s)
- Application server(s)
- Cache
- Search
- Custom

Project server
- In 2013 this was a bad experience and not a lot of fun
- In 2016 this is embedded in SharePoint 2016. it is implemented as a proper service application through Central Administration

Logic planning
- You need to update your 14.0 site collections to 15 mode before detaching content databases
- If you do not do this the upgrade will break
- Leverage MinRole role-based topologies

What is MinRole?
- Role-based server topology
- MinRole is self-healing
- Adaptable

You can switch a machines MinRole function when needed

There is one guy in the audience that has a farm of 200 servers, even Todd and Jason where impressed

The roles that we have
- Front-end
  - Handles user requests, including page rendering, service applications, etc
- Application

-
  -
    - All the back-end requests, timer jobs, search crawls
  - Distributed cache
    - Runs distributed cache service
  - Search
    - Search services and components like index
- Single-server farm
  - Has all services on a single server
  - Does not have SQL Express
  - No more than 1 server in the farm
  - Good for the developers
- Custom
  - There are not a lot reasons to use this, mainly for 3rd party services that haven't integrated with MinRole yet

To be MinRole compliant you need 4 servers, one of each roles
With HA you need 2 of each so 8 servers
If you have one of each you have all functionality of SharePoint
This is the RTM version of MinRole

In feature pack 1 we have a mini-MinRole (Shared Roles) (full MinRole topology with 2 servers and HA with 4 servers)

- Front-end with distributed cache
- Application with search

This will be available in November
The Min-Role is not an installation thing, but a configuration thing when you add the server to the farm
You can probably upgrade your single server farm to a custom role farm to add servers

Medium minRole HA (6 servers)

- 2 Front-end
- 2 Distributed cache
- 2 application with search

Or

- 2 front-end with distributed cache
- 2 applications
- 2 search

Search Planning; 2 options the traditional SSA or the Cloud SSA. Also available for SharePoint 2013
With the Cloud SSA the index role is in the cloud, so you do not need the disk space for this machine
You also get Office Graph and Delve experience; to get results the user needs a license. The index can be up to 1TB at this moment

- Infrastructure design
  - Networking
    - Traffic isolation
      - Multiple NICs

- SQL performance
  - Pre-grow databases
    - Requires more space initially
    - Dramatic increase in performance
    - Databases like contiguous space
  - Auto-growth
    - Immediately change from 1m increments
    - Do not user "Grow by %" setting
    - 50-100m maximun growth per required
    - Schedule maintenance task to check size ^ grow in off peak hours as required
  - Instant File Initialization

        - Allows for faster execution
        - Does not fill that space with zeros (disk content is overwritten as new data is written to the files)
        - Log files cannot be initialized instantaneously
- You want to split your databases to separate disks. The tempDB is the most important
    - Sizing
        - Recommended top end for ContentDBs: 200GB
        - It can be 4TB; when for archiving there is no limit
        - Because it can it is probably not an good idea
    - Database instance isolation
        - Secure store database
        - Sharepoint core database
        - Content database
        - Search
        - Highly Transactional non-SharePoint DBs
    - Drawback to this isolation, you lose the central management in a single SQL Server Management Studio window

- SharePoint performance
    - Now your network, determine your topology based upon traffic and requirements
    - Load balancing your app tier
        - Know your load
        - Scale bases upon need, not perception
    - Keep performance testing, not only at a base. Using load testing to know your base line
    - Tools
        - Fiddler - free
        - Microsoft's Virtual Roundtrip Analyzer (VTRA) - free
        - FireFox, IE, Edge - free
        - Visual Studio Team Services - $$$
        - Silk Performer - $$$
        - HP LoadRunner - $$$

- Watch the video on Zero Downtime Patching -> link in the slides

Modern Authentication - How it works and what to do when it doesn't

vrijdag 30 september 2016 09:00

BRK3215

Tom Batcheler
Jonas Gunnemo

OAuth based authentication for Office clients
OAuth is started by Twitter and Ma.gnolia, Google
It is secure delegated access

It is supported by Office 2013 and 2016 on windows, Office 2016 on Mac
The full support overview is on the slide deck

https://blogs.technet.microsoft.com/office_sustained_engineering

The updates for office are now on a regular schedule for Office 2013
- Public updates
  - Every Month
- Security Updates
  - Patch Tuesday
  - Download on Microsoft update, download center and Microsoft catalog MSI, C2R
- Non-security updates
  - 1st Tuesday of the month
  - Download on Download center and Microsoft catalog MSI

For Office 2016
- MSI install
  - Public updates are updated every month on patch Tuesday
  - Non-security updates are updated every month on the 1st of the month
- C2R (Click to Run)
  - Three channels where you can get your updates from
    - Microsoft ring
    - First release ring
    - Public ring

Refresh Tokens is saved in the credential manager
Access token is saved in the registry

Outlook connects over mapi-http, RPC is not supported anymore
Some of the times in the requests are in seconds, this is the number of seconds since 1970
In the slides there are a lot of examples of requests where thing can go wrong.

When you have a problem, make sure you have updated your clients and your servers

Client access filter is possible, but it is not available with OAuth traffic
Conditional access policies must use Modern Authentication

Customer scenarios where authentication is going wrong and how to fix it
Modern auth not working
- Environment
  - Federated

Outlook 2013 and 2013

Problem

Outlook is not using Modern Authentication
Word and OneNote are not working either

Questions

What login screens do you see
ADFS, any login screens

Steps

1. Check if ADAL is enabled. HKCU\Software\Microsoft\Office\15/16.0\Common\identity\
   Dword: EnableADAL 0 / 1
   Tools: http://aka.ms/offcat
2. Check if tenant is enabled for adal with PowerShel

Solution

Enable tenant

Outlook Disconnected at startup

Environment

Federated, mailbox on Office 365
Outlook 2013
100K users

Problem

Starting Outlook did not work
Logoff and login in Word resolves it

What we know

The authentication flow is working for the first authentication
The refreshing of the token seems to not working

Steps

1. Fiddler; outlook logging and MSO logging
   enable logging creates a lot of logs.
   In the TCO log search for ADAL, if nothing found something is really broken. In this case there was an message in the log that there was an Error validating credentials.

Solution

Update MSO.dll because there was a bug in this file

Outlook 2016 works, outlook 2010 does not

Environment

POC, Federated
Outlook 2010 and 2016
40.000 users

Problem

Can't create profile in 2010
Can create profile in 2016

Steps

1. Check if ADAL is enabled
2. Does autodiscover work?

Solution

Update ADFS Claims Rules -> Link in the slide deck
Not correctly configured AD FS Trust

It is important that you know the workflows how the authentication flow works, this will give you a better change to fix the issues faster

Tools

An overview of the tools are in the slide deck
http://diagnostics.outlook.com Support and recovery assistant for Office 365
https://Testconnectivity.microsoft.com

Make sure your client and server environment is updated

Share corporate resources with your partners using Azure AD B2B collaboration

vrijdag 30 september 2016 10:40

BRK3108
Sarat Subramaniam (Program manager Azure Active Directory)

Shadow IT is big, 80% of the users are using some kind of non-approved SaaS application
These users are there to get their work done, with or without the help of IT.
The solution is to offer the tools that leads the path of least resistance
That is the role that Azure AD wants to play as the control plane.

Business to Business is important for 97% of our customers.
The current reality is that we have a lot of different applications, devices and environments

Azure AD B2B is still in public preview

> I the new blades in portal.azure.com you do not need to choose what type of account you want to add. It will detect itself. If you add a user with an external email the type will be set to 'guest'
> In the property 'source' there is a value where the users will be authenticating, a Microsoft account or a other directory
> To add Azure AD B2B users add them in the current portal, you do not need to create and upload the CSV files :-). The default invite lets him to the Azure Portal, that is something that should be different in my opinion.
> DO not use the UPN to determine if the user is an external user, use the user type for this. Use the PUID for this.
>
> When a custom domain is used for the invited user, there will be a directory created for that domain and the user will be prompted for a password and verification for that domain by sending an email with a verification code. This domain is then set as an email verified domain. An admin can update this to a DNS verified domain.
>
> When you enable MFA on an application, the B2B user get also a MFA challenge. This depends on the MFA implementation of the partner
>
> The focus for now is on adding users, in the feature it also will be possible to add a whole group from another company. This is the design state

Announcement

> Public preview: sharing API
>
> > This is in the beta endpoint https://graph.microsoft.com/beta/invitations
> > This has the user display name, invite email address, send an invite, CC, invite redirect URL, custom email body
> > The result of this request gives back the invite URL so you can send the invite yourself or with the custom invite URL
> > This works for both an organization and an Microsoft Account
> > For now this needs to run in an user account context, the app context is coming

AAD B2B powered by all Office 365 apps; a full overview and roadmap is in the slide deck

Access reviews of external users is now in planning

Upcoming capabilities

> Done

- Audit and reporting
- Invitation API
- MFA for guest, depends on the partner MF

Roadmap

- Identity and access management experience UX
- MFA for guests with non-Azure AD accounts
- MFA for guests with Azure AD without MFA

More on the slides

Join your Windows 10 devices to Azure AD for anywhere, anytime productivity

vrijdag 30 september 2016 12:30

BRK3330
Jairo Cadena (Senior Program Manager) @jairoC_AzureAD

In Windows 10 we have a Work Account witch is the Azure AD login or federated login
This will give Single Sign-on to Office 365, SaaS and enterprise apps
This is an evolving from the on-premises AD join with the promise that you have Single Sign-on for cloud applications.
For the user this also gives enterprise settings and work data across joined devices
The user can use Windows Hello for business to access websites and business applications without typing their password

When you use Intune you can add policies and ensure that users are only able to login when certain criteria are met.
When you joined your machine to Azure AD you can set policies on that machine. Azure AD notices when the machine is joined to Azure AD and will automatically sign you into Office 365.

When the user has added to your Azure AD you can sync this back into the on-premises AD. This will give true SSO. When you use Windows Server 2016 ADFS you even have SSO to other ADFS applications

You can get the benefits of Azure AD Domain join with on-premises AD joined PC's. This can be done by synchronizing the computers to Azure

How to control the access for only Azure AD Join
- In Azure AD management portal you can set form the Microsoft Intune for who Intune must manage the PC
- For the application Office 365 Application you can set device based policies.
  - Setting this to compliant means that Intune will determine if a machine is compliant

Deployment considerations
- Preparing devices for work with Azure AD
  - Domain joined devices and mobile devices have different requirements. These must be met before you can continue
  - There is an installer for non-windows 10 and windows server 2016 computers
- Preparing domain joined
  - Requirements
    - Service Connection Point for discovery
    - If federated, issuance transform rules for computer authentication upon registration
    - Windows Installer package for non-windows 10 / windows server 2016 computers (Windows 7, 8, 8.1, Server 2008R2, Server 2012 and Server 2012R2

  - Group policy for roll-out of automatic registration
    - Windows 10 anniversary update and Windows Server 2016 register without policy set
    - Windows 10 November 2015 Update requires the policy set to trigger registration
    - Windows 8.1 responds to policy, can also use Windows Installer package

  - Azure AD Connect
    - Help with requirements setup - with caveats!

Key for lifecycle management of computers and devices

Check if the machine is registered

```
Dsregcmd.exe /status
```

SCP need to be created for every forest that have computers
This is used for all versions of Windows

Issuance transformation rules in ADFS, this is done with the AAD Connect applications
Device write-back is possible.

Server 2016 ADFS is needed for Windows 10 authentication to cloud applications in SSO