Contoso - Solution Design Report



Solution Design Report

Prepared for

Contoso

3-Jun-15

Version Final

Prepared by

**Pavel Bansky**

ePoint Consultant

Contributors

**Rob Young (Litware)**

Revision and Signoff Sheet

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Author | Version | Change Reference |
| 22.10.2014 | Pavel Bansky | 0.5 | Initial version for reviews |
|  |  |  |  |
|  |  |  |  |

Reviewers

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version Approved | Company | Date |
| Allie Bellew |  | Company A |  |
| Pavel Bansky |  | Company B |  |
| Bonnie Kearney |  | Company A |  |
| Rob Young |  | Company B |  |
| Belinda Newman |  | Company A |  |
| Robin Counts |  | Company A |  |
| Dorene Paschke |  | Company B |  |

Table of Contents

[1 Overview on the solution design 5](#_Toc420418565)

[1.1 Applications in Office 365 6](#_Toc420418566)

[1.1.1 Contoso solutions 6](#_Toc420418567)

[1.1.2 3rd party solutions 7](#_Toc420418568)

[1.2 Office 365 transition plan status 7](#_Toc420418569)

[2 General Architecture 7](#_Toc420418570)

[2.1 Network design 7](#_Toc420418571)

[2.1.1 Network routing for Office 365 8](#_Toc420418572)

[2.1.2 Cross Internet Office 365 9](#_Toc420418573)

[2.1.3 Selective Internet Access Office 365 10](#_Toc420418574)

[2.2 Provider hosting environment options 11](#_Toc420418575)

[2.2.1 On premises app hosting 12](#_Toc420418576)

[2.2.2 Azure app hosting 12](#_Toc420418577)

[2.3 SAML and external access 12](#_Toc420418578)

[2.3.1 Claims to groups 13](#_Toc420418579)

[2.3.2 Pass through claims 14](#_Toc420418580)

[2.3.3 Business to business groups 15](#_Toc420418581)

[3 Solution transformation plan 15](#_Toc420418582)

[3.1 Custom access denied page 15](#_Toc420418583)

[3.2 Notification on the document review due date 17](#_Toc420418584)

[3.3 Branding 17](#_Toc420418585)

[3.4 Legacy Component 19](#_Toc420418586)

[3.5 Record Management 19](#_Toc420418587)

[3.6 Location finder 20](#_Toc420418588)

[3.7 Skill Finder 20](#_Toc420418589)

[3.8 Data Migration API 22](#_Toc420418590)

[3.9 Analytics 22](#_Toc420418591)

[4 Required customizations for app model 23](#_Toc420418592)

[5 App transition plan to Office 365 platform 24](#_Toc420418593)

1. Overview on the solution design

Only limited number of solutions will be allowed in the new Office 365 platform. This is due to additional out of the box capabilities available in SP2013, or because the functionality can be achieved using alternative approaches.

Following table lists the solutions to be transformed to the Office 365 platform. Other solutions (Content Migrator and News Notifications) will be retired and replaced using out of the box capabilities.

|  |  |  |
| --- | --- | --- |
| Solution | Technical package | Notes |
| Safety News | contoso.sharepoint.safetynews.wsp | Displays safety news articles from all sites and sub-sites. Safety news will be created using Yammer announcements. |
| Branding | contoso.sharepoint.branding.wsp | Used to apply consistent branding to all the sites and sub-sites. Technique to apply the branding will be completely recreated to align with recommendations. |
| Records Management | contoso.sharepoint.docretention.wsp | Used to create lists and libraries for document retention. Solution also includes a timer job that provisions sub-sites. Contoso will use the SharePoint out of box document retention features. Lists and libraries will be created using CSOM API. |
| Provisioning | contoso.sharepoint.provisioning.wsp | Used to provision sub-sites, lists and libraries. Remote provisioning techniques will replace the full trust solution. |
| Event Receivers | contoso.sharepoint.libraryreceivers.wsp | Invokes business rule when user updates a list item or creates a site. The event handling will be implemented using remote event receivers. |
| Location Finder | fabrikam.locationfinder.wsp | The solution is used to search for Fabrikam outlets by Zip Code  The solution will be replaced by SharePoint search with display templates |
| Skill Finder | tailspin.skillfinder.wsp | The solution allows users to “search” experts based on their skills, years of experience and past projects.  The solution will be replaced by SharePoint search with display templates |
| Analytics | adventureworks.analytics.wsp | The solution offers granular insights into the usage patterns and user access.  The solution will be replaced by SharePoint 2013 analytics and other JavaScript injection techniques. |

These solutions will be built using agreed app model standards. The process will be documented for Contoso. These standards are categorized with following categories. Each category contains high-level design principles and solution design patterns to be used in future development.

* 1. Applications in Office 365

Contoso has decided to move to Office 365 multi tenant platform . Following chapters lists the currently existing farm solution in the Office 365 farm group based on the ownership. This is the full list of solutions that were analyzed as part of the assessment phase. Specific action plan has been defined for each of the solutions. A detailed description of the required steps is provided later in this document.

* + 1. Contoso solutions

Following table lists the existing Contoso solutions and describes the transition plan for the next stages.

|  |  |  |  |
| --- | --- | --- | --- |
| Solution | At Present | Office 365 | Description on the actions |
| contoso.sharepoint.safetynews.wsp | Yes | No | Not transferred to the Office 365 platform. Replaced with Yammer functionality using embedded Yammer code. Every department and unit will have its own Yammer group |
| contoso.sharepoint.branding.wsp | Yes | Yes | Alternative and more simplified approach to provide consistent user experience will be adopted. |
| contoso.sharepoint.provisioning.wsp | Yes | Yes | Alternative and more simplified approach to provision sub-sites and lists will be adopted. |
| contoso.sharepoint.docretention.wsp | Yes | Partly | Contoso has agreed to stay with the features that can be offered using the native Office 365 eDiscovery and data management capabilities. |
| contoso.sharepoint.libraryreceivers.wsp | Yes | Partly | Contoso needs to assess the value of this functionality internally. Most of the functionality can be achieved using remote event receiver techniques |
| contoso.sharepoint.newsalerts.wsp | Yes | No | Not transferred to the Office 365 platform. Replaced with Yammer. |

* + 1. 3rd party solutions

|  |  |  |  |
| --- | --- | --- | --- |
| Solution | At Present | Office 365 | Description on the actions |
| tailspin.skillfinder.wsp | Yes | Yes | This functionality can be achieved using SharePoint 2013 search and display templates |
| wingtip.migrationhelper.wsp | Yes | No | Old solution, which will be retired. Other third party solutions will be evaluated which do not require installation on SharePoint farm. |
| adventureworks.analytics.wsp | Yes | Partly | SharePoint Reporting and other client side JS injection techniques will address most of the requirements |
| fabikam.locationfinder.wsp | Yes | Yes | This functionality can be achieved using SharePoint 2013 search and display templates |

* 1. Office 365 transition plan status

Currently only the Branding solution has clear transition plan. The same was reviewed during this assessment. Other solutions are awaiting for input from Contoso IT team.

There are some critical decisions, that will directly impact on the customization architecture, like following

* App model hosting structure for Office 365
  + App hosting will be done in on-premises
* Network level architecture for Office 365 service
  + Will cross Internet traffic be allowed or will the traffic be routed through on-premises network using secure reverse proxies and MPLS links

1. General Architecture
   1. Network design

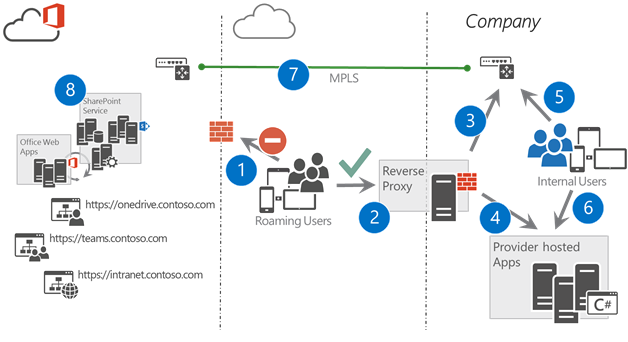
Network design principles has direct impact on the app model hosting decision. In higher level there are two main approaches, with multiple variations. Users are either routed to the Office 365 platform cross Internet or through MPLS link with corporate network.

Recommendation is to use the cross internet design model to gain maximum value for the service. This will ensure that also different devices which might not be in the corporate network can also access services and information hosted in the Office 365 platform.

* + 1. Network routing for Office 365

Since the app model customizations are required to be exposed for partners and also for roaming internal users, there are network level changes required for each of the specific provider hosted apps, which are planned to be used in the Office 365 platform.

Following picture is showing the logical routing of the environment where network connectivity to Office 365 is routed cross-corporate network and the app model hosting is setup to on-premises.



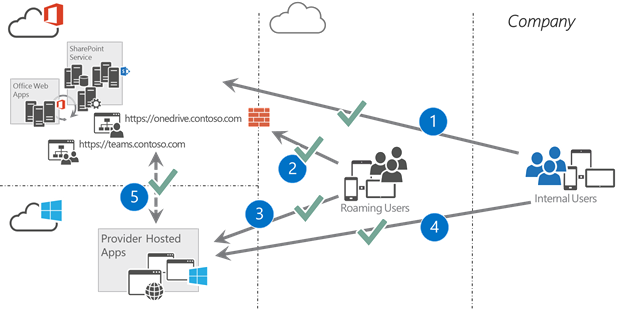
1. Cross Internet access is not available for roaming internal users or partners
2. All traffic from outside of the corporate network is routed to secure reverse proxy, which is used for authentication of the user
3. SharePoint or Office 365 faced traffic is routed using MPLS link between corporate network and Microsoft data center
4. Since cross internet access is not enabled, provider hosted apps will need to be hosted in on-premises.
   1. Typical .NET platform with corporate SLAs and operations
5. Users in corporate network are routed to the SharePoint or Office 365 side using MPLS link
6. Users in corporate network can access the provider hosted environments directly
7. MPLS link is securing the traffic between corporate network and the Microsoft data center
8. SharePoint and other Office 365 services are hosted in the Microsoft data center

This model has some functional and operational challenges, which should be considered when hosting decision is done for the Office 365 platform.

* Any provider hosted app which is developed, will need to be published from the reverse proxy to avoid issues with limited capabilities for people accessing services from Internet
* Native apps from different platforms (IPad, Android, Windows Phone) cannot access the services and content in the Office 365, since they do not support network routing cross secure revers proxies.
  + 1. Cross Internet Office 365

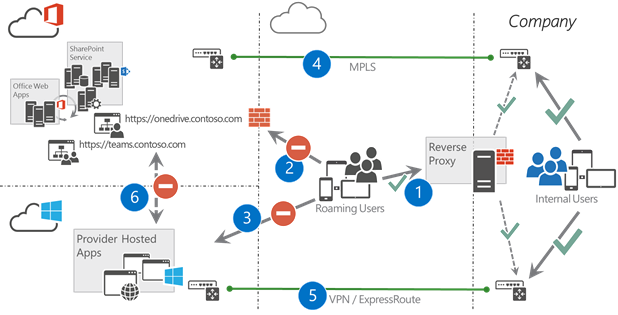
This is the recommended option where the traffic is routed cross internet to Office 365. This provides the most flexible environment for difference devices, regardless of their location, meaning that all the native apps and services are fully supported with any device. Model also ensures the recommended way to utilize Microsoft Azure as the hosting platform for provider hosted apps without any additional complexity. This means that customers can take advantage of the Platform-as-a-Services capabilities without any additional overhead of managing actual virtual machines.

All authentication to Office 365 service will still happen using designated devices in customer network. In the case of Contoso, FAAS will be used to as the authentication provider for the Office 365.



1. Traffic from users in the corporate network is routed directly over the Internet towards the Office 365. All requests are authenticated using ADFS (or other identity provider) to secure the traffic
2. Roaming users can access all the services with any device as long as they have Internet connectivity. This provides easy access to the services and documents regardless of their physical location
3. Provider hosted environment in Microsoft Azure PaaS platform for difference apps and other customizations. Access is commonly secured with the oAuth tokens from the Office 365 side.
4. Users in corporate network can access the Azure services also cross Internet
5. Provider hosted apps in the Azure can connect the different services in the Office 365 directly in the cloud. Authentication and authorization will by default happen using the oAuth tokens.
   * 1. Selective Internet Access Office 365

Office 365 platform can be also secured from cross Internet access, if that is needed due company policies. This option will however influence negatively on supported capabilities in the platform. Model would for example block any native app access from different devices to the services and documents stored in Office 365 platform.



1. Roaming users are routed to the service using secure reverse proxy hosted in on-premises environment
2. Direct access to Office 365 services is denied with selective Internet access
3. Users could access the Azure capabilities, but those apps would not have access to corporate resources or Office 365 if the traffic is routed cross Internet
4. Actual Office 365 traffic from Internet and corporate network is routed cross MPLS link between corporate network and Microsoft data center
5. All Azure traffic is routed using point to point VPN or by using ExpressRoute. This capability however is only supported for limited set of functionalities in Azure platform, which will limit the capabilities in the app platform
6. There is by default no direct access from the Azure to Office 365. This traffic is either routed from the Azure through on-premises network or by using selective Internet traffic between Azure and Office 365. This selective internet traffic option between Office 365 and Azure is only supported for limited set of capabilities in the Azure.

This is extremely complex network layout and will have significant influence on releasing new capabilities in the Office 365 platform by causing significant operational burden for the on—premises teams.

* 1. Provider hosting environment options

Chosen hosting platform is highly dependent on the network security polices and if the cross Internet traffic is enabled or not. We strongly recommend to use Azure as the default options for hosting platform. All future development effort and samples will be more towards the Azure based implementation, rather than on-premises.

* + 1. On premises app hosting

On-premises hosting is needed if cross Internet access to Office 365 is not allowed. These services can be also hosted in some IAAS provider as long as the machines are either explicitly part of the corporate network or there is existing routing to Office 365 from the servers.

* + 1. Azure app hosting

Following table shows the current options related on the Azure based hosting and the dependency between different capabilities on the network level configuration. It’s important to notice that the default provider hosted app model in Azure would be using the Azure Web Sites option.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Azure VPN/ExpressRoute | Selective Internet access | Public internet |
| Azure Web Sites | Yes | No (\*) | Yes |
| Azure Cloud Services | Yes | Yes | Yes |

Azure web sites not have static IP addresses for outbound traffic which is making them not to be the proper option in case of Selective Internet access. The addresses are coming from a pool of addresses. Selective internet access would mean whitelisting the whole range and thus also allowing other Azure web sites to reach SharePoint

* 1. SAML and external access

Contoso has SAML based users accessing the services in the cloud and in the upcoming Office 365 platform. Currently there are significant amount of full trust code customizations to enable external partner access. These customizations will be replaced with out of the box capabilities that will be introduced to the Office 365 platform.

It is important to notice that each user who is accessing SharePoint Online services will need to have Azure active directory identity. On top of this identity management, we can also use specific claims for setting permissions in the service. Whenever the user has been authenticated, actual customizations will work seamlessly regardless on how the user was authenticated.

Different options introduced in following chapters can be combined for different scenarios.

* + 1. Claims to groups

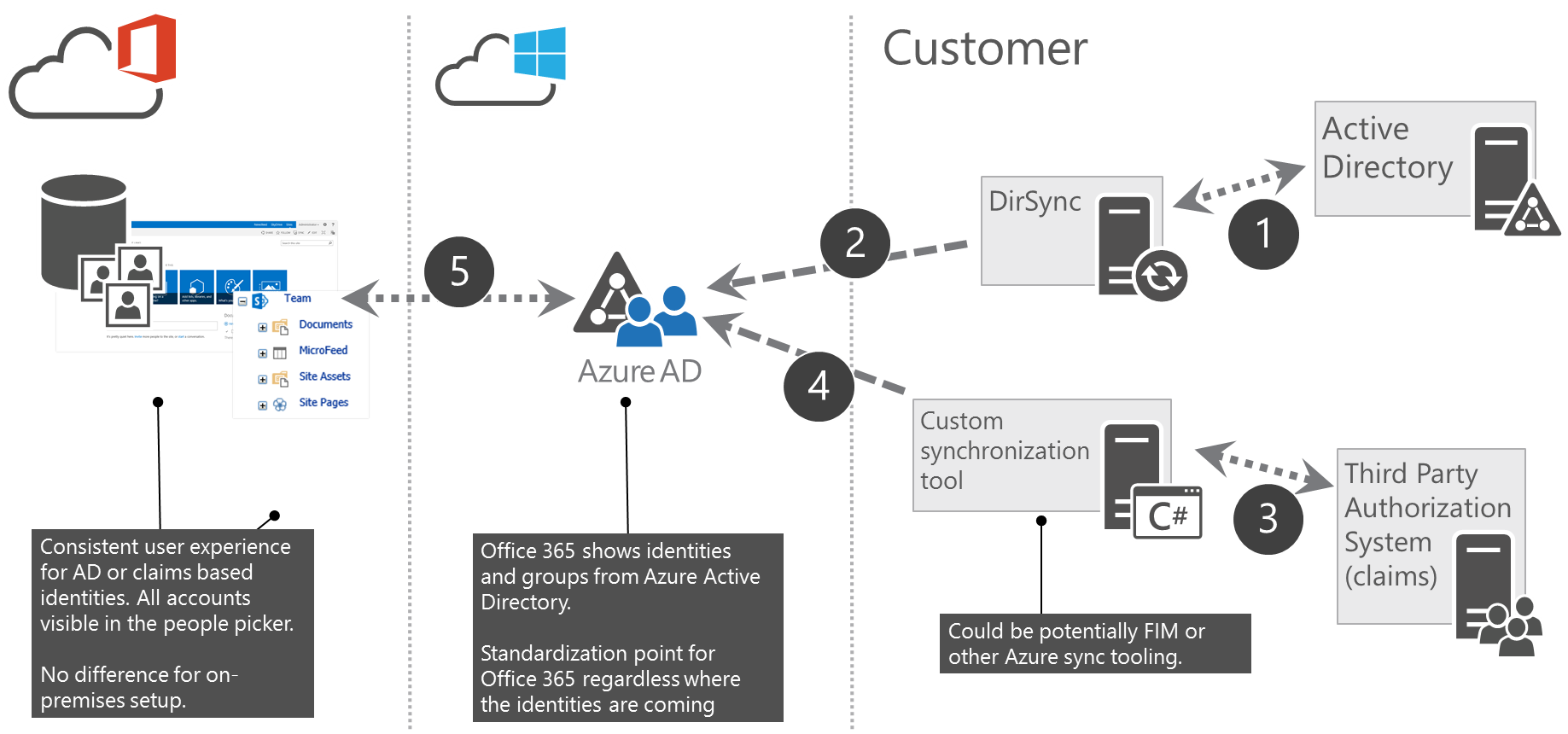
This is already existing model where the different claims in 3rd partly identity system are being used to created security groups to Azure Active Directory and the partner identity is being assigned to these groups. These partner identities have to be created as identities to the on-premises AD or directly to Azure AD.

Advantages of this transformation is that the AD groups can be used to manage permissions without any changes in the SharePoint online. This means that the groups will be available for assigning permissions in the native SharePoint site permission management. Challenge of this option is however that the replication of changes performed in the 3rd party identity system can take a while.

This pattern has not been verified and is assuming that FIM or a custom synchronization engine can dynamically create groups to the Azure platform as needed.

Model is usable for scenarios like

* Let’s give permission for all identities from Litware company which has identity in our active directory
* Let’s give permissions to all external users in our active directory



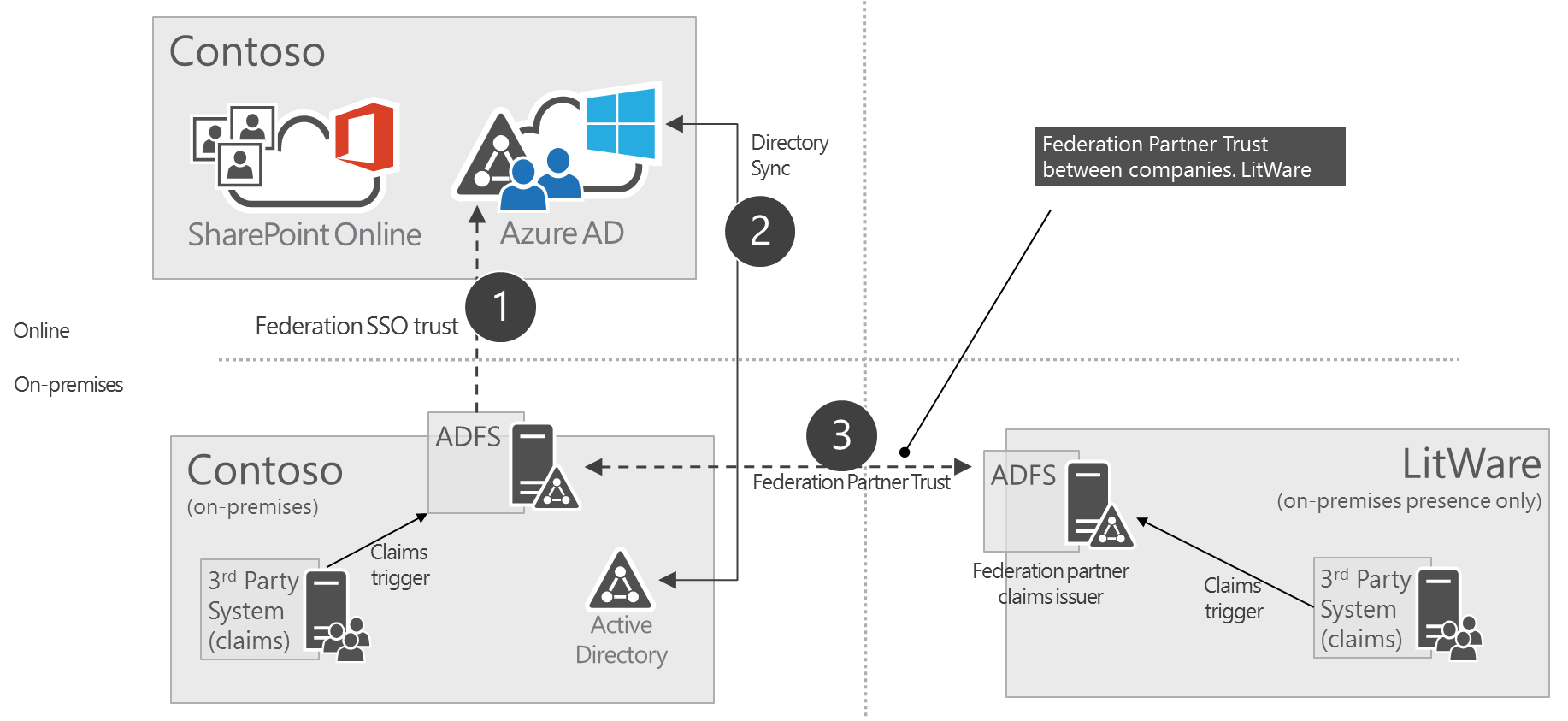
1. Normal AD connection
2. DirSync for replicating the accounts from on-premises to Azure
3. 3rd partly authorization system which contains the needed claims to be configured
4. Connection to create the needed AD groups. Could be potentially FIM or other sync tool
5. SharePoint is associated to Azure AD for the permission management. You can assign permission using the groups in the Azure AD
   * 1. Pass through claims

This model gives opportunity to assign permission in the SharePoint online using specific claims. These claims can be configured in the SharePoint online side and they are exposed as resolved identities through people picker.

When users are authenticating towards Office 365, they can be given access to specific resources based on claim which is augmented to user session. User does not need to have identity in the customer Azure AD to be able to gain access to assets.

Scenarios where this approach could be taken:

* Give access to all external users to specific capability
* Give access to all internal users based on claim (if internal users are using same system)
* Control access to specific site based on partnership level which is controlled in different third party system, but exposed to be available during authentication

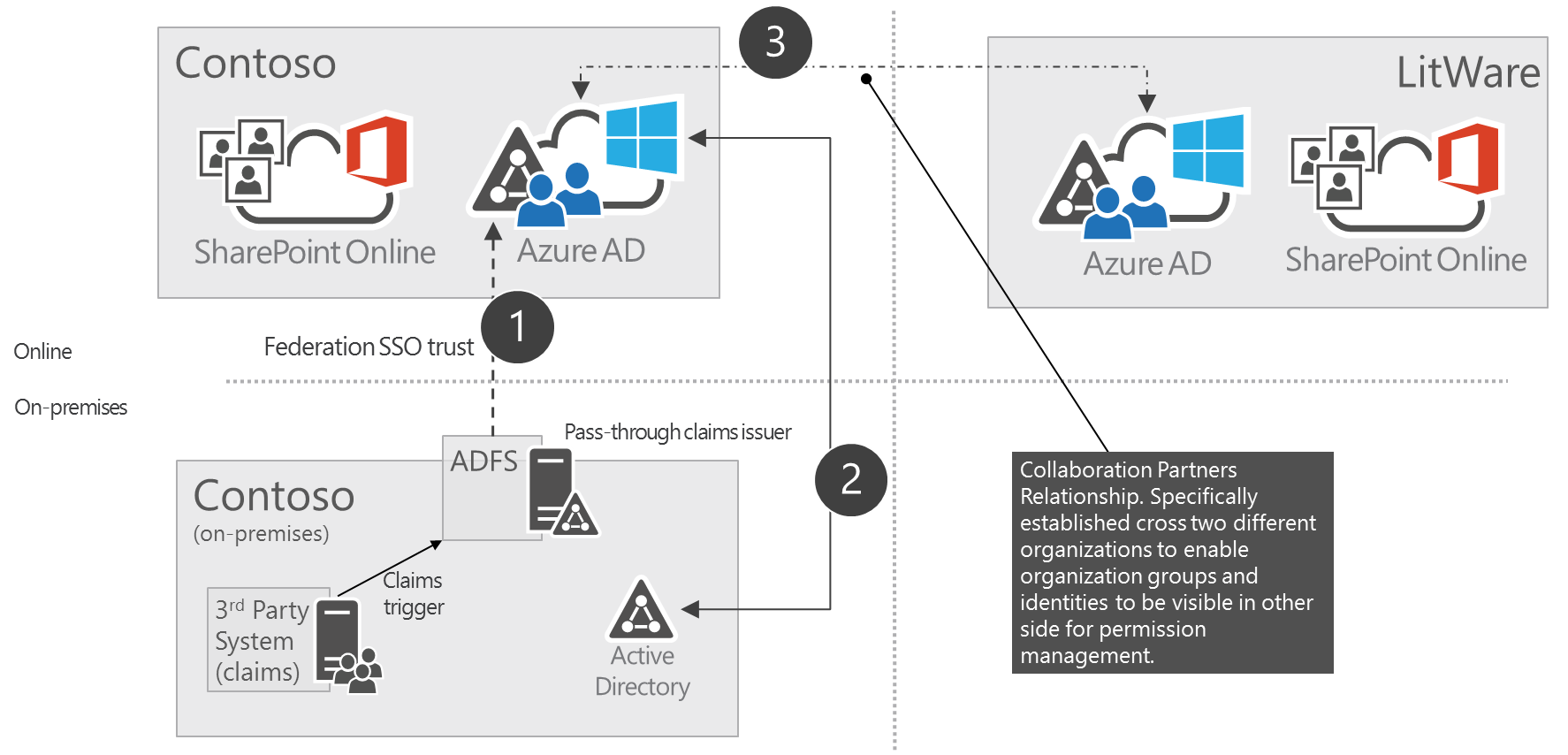


1. Normal SSO trust between on-premises and Azure
2. Identity sync’d to cloud
3. Federation partner trust to provide access on trusted accounts
   * 1. Business to business groups

This model gives opportunity to assign group based access to the SharePoint online assets by using groups from other companies Azure AD. This gives opportunity to directly assign permissions using existing groups and authorization from partner Azure AD. Trust can be specifically established with the customer and partner companies.

This model is suitable for following scenarios

* Assign permissions to access specific partner site for all users in the partner organization
* Assign permission to project sites using specific organizational groups from partner AD which will be managed by the partner
* Delegate the responsibility to manage permission to partner organization

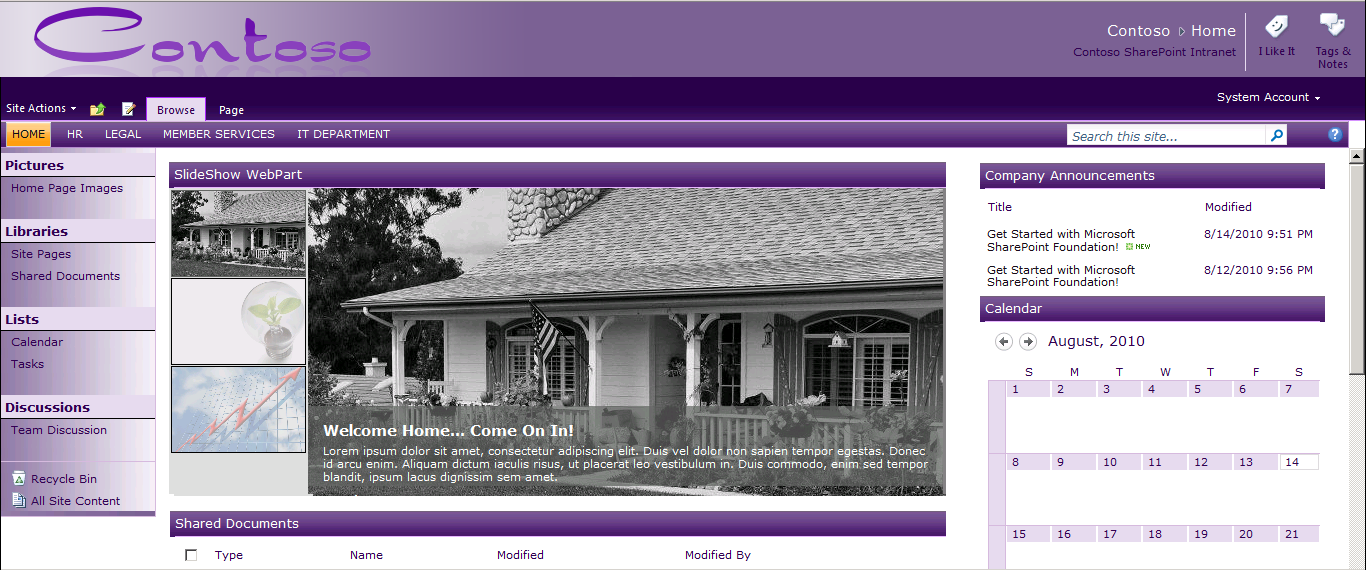


1. SSO trust for customer users
2. AD sync to Azure AD for identity mapping
3. Actual trust established with the partner organization to set permissions directly based on the ad groups from partner AD
4. Solution transformation plan
   1. Branding

**Solution name:** contoso.sharepoint.branding.wsp

Provides consistent branding using custom master page, which is applied to each site type when they are created. Currently implemented using feature stapling technique in farm scope, which cannot be achieved in the Office 365 platform.

Following picture shows the branding applied to normal team site.



Implementation will be completely changed for the Office 365 platform to align with Office 365 recommendations. This means that the branding will not be applied using custom master page to avoid issues with future updates which would not be automatically applied to custom master pages. This will ensure that sites will receive any out of the box updates to the user interface automatically, which will reduce overall maintenance costs related on the branding elements and future updates.

Implementation will be updated to be based on following elements

* Custom theme to provide Contoso specific colors and fonts
* Custom CSS to perform optional additional alignment with the layouts and styles
* JS injection based implementation for the needed header and footer implementation

Following picture shows the specific UI level configurations which are being applied using JS injection technique.

As part of this redesign, the layout will also be changed to avoid issues with constantly evolving suite navigation. Actual design has not been finalized, but the top header navigation elements should not be placed inside of the suite navigation area, since that is consistent cross other Office 365 services.

A custom spcolor file will be generated with the blue theme in mind. This will be followed by a new Composed look item which will reference the Oslo masterpage and the spcolor file we created above. Final tweaks to the alignment of controls will be performed using an alternate CSS file.

These artefacts will be uploaded to SharePoint using a provider hosted app using provisioning techniques explained later.



1. Suite navigation area which is same cross Office 365 services (Delve, Sites, Yammer etc.) and not only specific for SharePoint Sites. Color will be controlled centrally from the tenant administration site of the Office 365 tenant.
2. Contoso and SharePoint specific header with cross site collection links, which are static implemented using JS Injection technique
3. Footer with some dynamic elements based on user profile. Implemented to SharePoint sites using JS injection technique

Above customizations are implemented using JS injection technique by attaching needed JavaScript file to the page-processing pipeline by using user custom actions. This way there is no need to implement a custom master page, but the required elements could still be rendered in the page. It is also important to pay attention on proper client side caching to minimize any delays for showing the needed elements in the page.

App model will also be used to create publishing pages and adding webparts on them. To provision Publishing Page your app requires the Write permission on the Web where the page is to be created. Additionally, if your app is installed in a subweb to create pages there, it will also need the Read permission on the Site Collection in order for it to retrieve the Page Layout to be used to create the page.

Provisioning preconfigured Web Parts to pages can be also accomplished using the App Model.

The web part XML is added on the provisioned page using the CSOM techniques.

.

* 1. Legacy Component

**Solution name:** contoso.sharepoint.solution7.wsp, contoso.sharepoint.solution8.wsp

These solutions are not in use currently. They will be removed from the farm.

* 1. Safety News Features

**Solution name:** contoso.sharepoint.safetynews.wsp, contoso.sharepoint.newsalerts.wsp

Contoso is very particular about Safety at Workplace.

All safety incidents reported at various units are logged into the Safety List for the specific site. Every site has safety news displayed on the homepage through a safety web part.

In addition to showing the safety incidents for the unit/department, the webpart can also pulls safety incidents raised in other departments.

The design of the solution will be changed completely. Instead of tracking the news items on every site, the news articles will be created on Yammer. Every unit and department is going to have a Yammer group.

The safety news is going to be added on the site homepage using Yammer embedded code.

User will few safety news from all departments he subscribes to.

Given the importance of safety at Contoso, major safety incidents will be created as announcements. Yammer sends email notifications every time an announcement is added.

Yammer mobile app can be used to view the safety news on mobile without any additional customization or effort.

Users can also share the safety articles with colleagues using Yammer

* 1. Provisioning

**Solution name:** contoso.sharepoint.provisioning.wsp

Contoso has a provisioning framework that allows self-service site provisioning through a custom full trust solution.

The same can be implemented using the App model techniques.

Remote provisioning is model where the template is built using provider hosted pattern to provide customizable sub site creation experience for the end users of the SharePoint.

Benefits of the remote provisioning model is that one doesn’t need to have any feature framework elements or other customizations deployed to SharePoint farm, rather they can control the customizations outside of the SharePoint, which gives the ability to update and change the provisioning engine without any impact on SharePoint side from availability perspective.

|  |  |
| --- | --- |
|  | **Additional Information** |
| *Following blog post is showing the recommended technique to be used with the site provisioning.*   * [Site provisioning in Office 365](http://blogs.msdn.com/b/vesku/archive/2013/08/23/site-provisioning-techniques-and-remote-provisioning-in-sharepoint-2013.aspx) | |

Similar app provisioning techniques will be used to deploy the custom theme (spcolor file) and alternate stylesheet to the SharePoint site.

|  |  |
| --- | --- |
|  | **Additional Information** |
| *Following blog post is showing the recommended technique to be used to deploy site artefacts.*   * [Upload and Change Alternate CSS in Office 365](https://github.com/OfficeDev/PnP/tree/master/Samples/Branding.AlternateCSSAndSiteLogo) | |

* 1. Record Management

**Solution name:** contoso.sharepoint.docretention.wsp

Used to send automated emails when a document has reached the review date. It also deletes the documents that are over 7 years old and logs the deletion information in a SharePoint list.

All of the functionality that require full trust code in farm, can be achieved in the Office 365 platform using alternative means. Following table definite, the new approach for the Office 365 implementation.

|  |  |  |  |
| --- | --- | --- | --- |
| **Functionality** | **At Present** | **Office 365** | **Notes** |
| Set the site collection owner and secondary contact | Yes | Yes | Can be achieved with CSOM |
| Set retention policies | Yes | Yes | Can be controlled with document deletion polices in Office 365. See more about [Default MRM Policy](http://blogs.office.com/2015/02/20/extended-email-retention-deleted-items-office-365/) |
| Set audit settings | Yes | Yes | Will be available as setting from tenant administration tooling. No need to set in site collection level. |
| Configure Document Set Template  (shared fields and allowed content types) | Yes | Yes | Exposed as remote API using CSOM. |
| Configure Document Set Template (shared fields) | Yes | Yes | Exposed as remote API using CSOM. |

* 1. Event Handling

**Solution name**: contoso.sharepoint.eventreceivers.wsp

Event handling has been implemented to handle security after a site is provisioned or deleted. It has also been used to update the metadata of a document after it is uploaded. Creation of site columns and content types has also been performed using feature receivers.

This procedural code is currently loaded from a .NET assembly found in the Global Assembly Cache (GAC) on the SharePoint server. To be CAM compatible this code will be relocated to a remote hosting location and refactored into a **Remote Event Receiver** which uses CSOM or REST interfaces to communicate back to SharePoint. Additionally, all synchronous event receivers (ex: WebAdding, ItemUpdating, SiteDeleting) will be re-coded as asynchronous event receivers (ex: WebProvisioned, ItemUpdated, SiteDeleted) as Remote Event Receivers are exclusively asynchronous. This implies the developer no longer has the ability to “cancel” an event, as they are only called after the event is complete.

**Feature Receivers** are being used to perform additional provisioning or setup/cleanup on the current site collection or web as a feature is activated or deactivated. For example, creating groups or adding the Content Editor Web Part to the NewForm.aspx or EditForm.aspx on the Request list. Similar site provisioning work will be done using an **App Event Receiver** included in a **Provider Hosted App**

* 1. Location finder

**Solution name:** fabrikam.locationfinder.wsp

The full trust solution allows the users to search for Fabirkam locations and provides an interactive map to browse through the locations.

Same functionality will be provided using SharePoint search and display templates. App provision techniques described above will be used to upload display templates to Office 365.

* 1. Skill Finder

**Solution name:** tailspin.skillfinder.wsp

Allow users to search experts based on their years of experience and past projects.

SharePoint People search and display templates will provide the same functionality.

SharePoint People search offers Lync integration, which will allow users to contact the subject matter experts instantly.

App provision techniques described above will be used to upload display templates to Office 365.

* 1. Content Migrator

**Solution name**: wingtip.migrationhelper.wsp

Contoso will use a third party product (Northwind Migration Suite) to migrate data and content within SharePoint farms and site collections. The tool uses the SharePoint web services and does not require an installation on the SharePoint servers. It also allows operational and administrative capabilities.

* 1. Analytics

**Solution name**: adventureworks.analytics.wsp

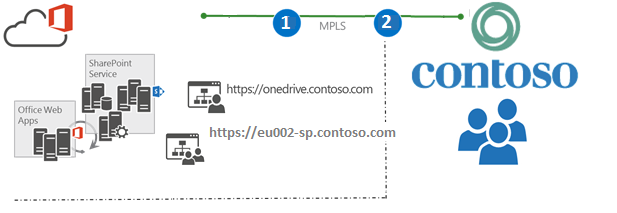
For most cases, Contoso will refer to the out of box SharePoint Analytics Usage Reports.

For special cases, Contoso will use a custom JavaScript to extract usage statistics. The JavaScript will be placed in a script editor webpart on the page layout.

App provision techniques described above will be used to upload the JavaScript to Office 365.

**If App model solution is not delivered on time**

In this case, the MS Toolkit will not be relocated to the Office 365 like other solutions. The app will have to be deployed on the on-premises platform.



1. Users accessing the old farm will happen using the MPLS link. This will ensure that the solutions which are not ready to be moved, can still remain in the old platform until they are transferred to the app model based techniques
2. The services that could not be transformed in the Office 365 platform will be accessed from the Contoso network. All other services will be relocated to this platform to get benefits on most up to date capabilities

**If App model solution is made available on time**

If app model solution is delivered on time, transition to the Office 365 will be performed after the content is migrated to new app model based solution.

1. Required customizations for app model

As a general guidance for the app model transition, we recommend concentration on following main topics, which each should have specific patterns and guidance for development projects.

* **Provisioning Framework**
  + Should be one solution which is used for site collection and sub site creation in consistent way. Individual projects can provide difference configurations and assets to be applied to sites.
  + All operations to be applied using CSOM or remote techniques. No references to feature framework elements (declarative deployment)
* **Remote Timer Framework**
  + Generic provider hosted guidance for scheduled task executions, which is needed to replace classic timer jobs
  + Standardized guidance on how to implement
  + Guidance on the account usage: when to use service account and when to use app only tokens.
* **Branding and Asset Framework**
  + Guidance on how to handle required branding and other assets that are to be deployed to the sites. Where content should be placed and how it is maintained.
  + Process and tooling for handling updates on the branding elements across existing sites.
* **Development Framework**
  + Guidance on the hosting platform usage and not to address difference scenarios, like connections to on-premises LOB systems.
  + General design guidance for provider hosted apps on typical implementation guidance like logging and caching.
* **Transformation Framework**
  + General design approach to remove FTC solutions from the existing sites
  + Transformation tooling, like updating existing master pages or transforming custom list templates to new app model supported formats

|  |  |
| --- | --- |
|  | **Note** |
| *Office 365 Developer Patterns and Practice project is about to be release more detailed guidance and input on above topics. These will be available from the Office 365 Patterns and Practices GitHub project.*   * [*Office 365 PnP GitHub*](https://github.com/OfficeDev/PnP) | |

1. App transition plan to Office 365 platform

Following table is listing the high level transition plans for different kind of elements in the Contoso environment.

|  |  |
| --- | --- |
| Element | Transition plan |
| Module | Deploy newer version of the file, like custom page layout, with different name. Scan through sites to associate the new file.  If this is not possible, you can un-ghost the module file before feature responsible for the deployment is deactivated. |
| List Definition | Data from existing lists will have to be migrated to out of the box list, which can then be customized based on the list definition details.   1. Export list data 2. Delete existing list 3. Create new list instance using OOB template 4. Apply needed changes to the list instance 5. Import list data   3rd party migration tool might be used. Community tooling solution also in progress. |
| List Template | Refers to legacy list templates which are still using the stp format. These will work as such also in non-FTC deployments. |
| Site / Web Template | Site or web template is only required during initial site creation. There will not be any reference on actual onet.xml file after the site has been created.  Individual features and their element files will however need to be converted one by one. This is where the specific guidance for feature framework elements should be followed. |
| Workflow | Custom SP2010 workflows cannot be converted to 2013 format. Each workflow will have to be re-created in new format. All existing running instances of the workflow should be stopped or deleted before the workflow code is retracted from the farm. |
| Delegate Control | Will have to be replaced using client side techniques either directly in the master page or by using JS injection pattern. |
| Field Control | Will have to be replaced using client side techniques either directly in the master page or by using JS injection pattern. |
| Field Type | Will require full content migration to ensure that content has no dependencies on the custom field type implementations. |
| Timer Job | Will have to be converted to remote timer job format. All existing instances of the custom timer jobs need to be deleted before the full trust code is removed from the farm. |
| Event Receivers | Will have to be converted either to remote event receivers or workflow logic. If the custom code execution does not have to be instant, remote timer job might be a solution.  Alternative ways to achieve the needed end result should be pursued, since remote event receivers are not as reliable as the server side event receivers. |
| Custom Features | All custom features will need to be deactivated explicitly from the existing sites before full trust solutions are retracted from the farm. |