Contoso - Solution Design Report



Solution Design Report

Prepared for

Contoso

5-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 |  | Contoso |  |
| Pavel Bansky |  | Litware Inc |  |
| Bonnie Kearney |  | Contoso |  |
| Rob Young |  | Litware Inc |  |
| Belinda Newman |  | Contoso |  |
| Robin Counts |  | Contoso |  |
| Dorene Paschke |  | Litware Inc |  |

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

On the new Office 365 platform, only some of the existing customization will be required. This is due to additional out of the box capabilities available in SP2013, or because the functionality can be achieved using alternative approaches.

The following table lists the existing SharePoint Solutions that contain functionality that is required on the Office 365 platform. Solutions not listed here, 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. In order to align with recommendations the branding provisioning tools will be re-developed. |
| 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.  SharePoint 2013 analytics and other JavaScript injection techniques will replace the existing solution. |

Development will user agreed app model standards when building the replacement for these solutions. Contoso will receive documentation of the process followed.

* 1. Applications in Office 365

Contoso has decided to move to the Office 365 platform. The following section lists the SharePoint Solution currently deployed within the Contoso on premises SharePoint farm. In the assessment phase Litware performed analysis of the following solutions. Each solution has had a specific action plan defined. This document provides a detailed description of the required steps.

* + 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 | Adopt an alternative and more simplified approach to provide consistent user experience. |
| contoso.sharepoint.provisioning.wsp | Yes | Yes | Adopted alternative and more simplified approach to provision sub-sites and lists. |
| contoso.sharepoint.docretention.wsp | Yes | Partly | Contoso has agreed to stay with the features that offered by 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 a clear transition plan. Other solutions are awaiting for input from Contoso IT team.

There are some critical decisions that will directly influence the customization architecture, such as the 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

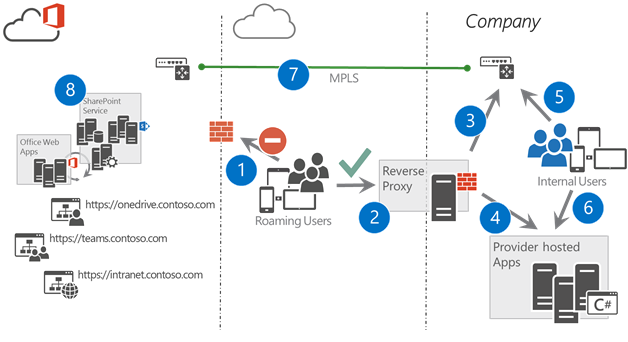
Network design principles has direct impact on the app model hosting decision. At a high level, there are two main approaches, with multiple variations. Network traffic to the Office 365 platform travels either cross internet or through MPLS link with corporate network.

The cross internet design is the preferred approach in order to gain maximum value from the Office 365 service. This will ensure that also different devices can access services and information hosted in the Office 365 platform while they are not on the corporate network.

* + 1. Network routing for Office 365

Contoso require that the App Model customizations are available to partners and roaming internal users. As such, there are network level changes required for each of the planned provider hosted apps for 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.



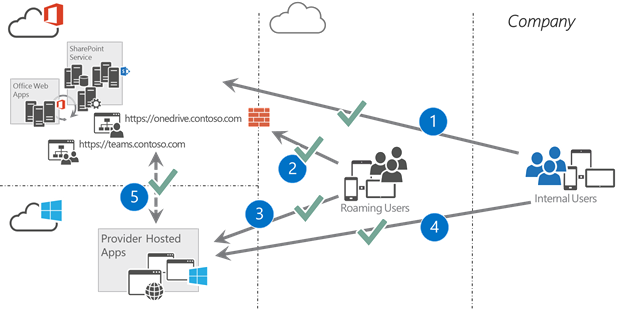
1. Cross Internet access is not available for roaming internal users or partners
2. All traffic from outside of the corporate network is routed to secure reverse proxy, which is used for authentication of the user
3. SharePoint or Office 365 faced traffic is routed using MPLS link between corporate network 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

When making the hosting decision for the Office 365 platform there functional and operational challenges of this model to be considered.

* 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, and Windows Phone) cannot access the services and content in the Office 365, since they do not support network routing across secure reverse proxies.
  + 1. Cross Internet Office 365

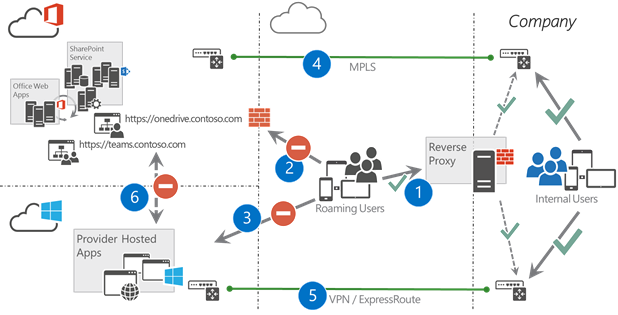
This is the recommended approach. Routing of network traffic to Office 365 goes across the internet. This provides the most flexible environment for difference devices, regardless of their location. This ensures full support for all the native apps and services on any device. Model also ensures the recommended 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, ADFS will be the authentication provider for the Office 365.



1. Traffic from users in the corporate network travels directly over the Internet to 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 different apps and other customizations. OAuth tokens from Office 365 will secure access between systems.
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

It is possible to block cross Internet access to the Office 365 platform, if needed due company policies. This option will however influence negatively on supported capabilities in the platform. This 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 uses a point-to-point VPN or 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 from Azure goes via the on-premises network or by using selective Internet traffic between Azure and Office 365. There is support for a limited set of Azure capabilities when using the selective internet traffic option between Office 365 and 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

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

* + 1. On premises app hosting

If corporate policy prevents cross Internet access to Office 365 on-premises hosting is required. Contoso can host these services using an IAAS provider as long as the machines are either explicitly part of the corporate network or there is 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 is 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 |

In case of Selective Internet access, Azure Web Sites are not a viable option, as they do not have static IP addresses for outbound traffic. 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. This Office 365 platform provides out of the box capabilities to replace these customizations.

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 is authenticated, actual customizations will work seamlessly regardless of authentication mechanism used.

In different scenarios, it is appropriate to use different combinations of options as introduced in the following sections.

* + 1. Claims to groups

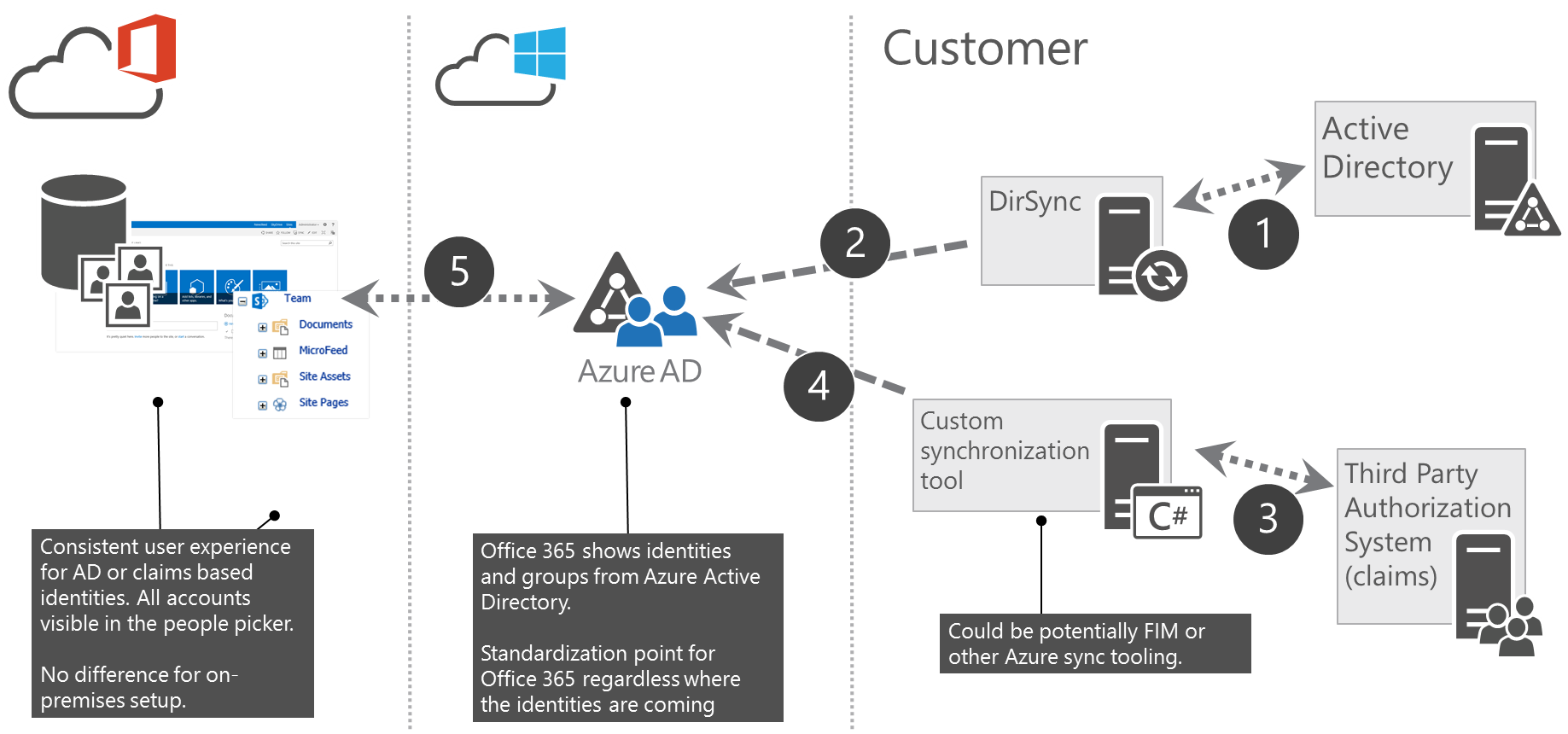
This is an already existing model where the different claims in 3rd partly identity system are being used to create security groups within Azure Active Directory and the partner identity is being assigned to these groups. In this scenario, Contoso will create these partner identities as identities within the on-premises AD or Azure AD.

Advantages of this transformation is management of permissions via AD groups 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 is unverified and assumes 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



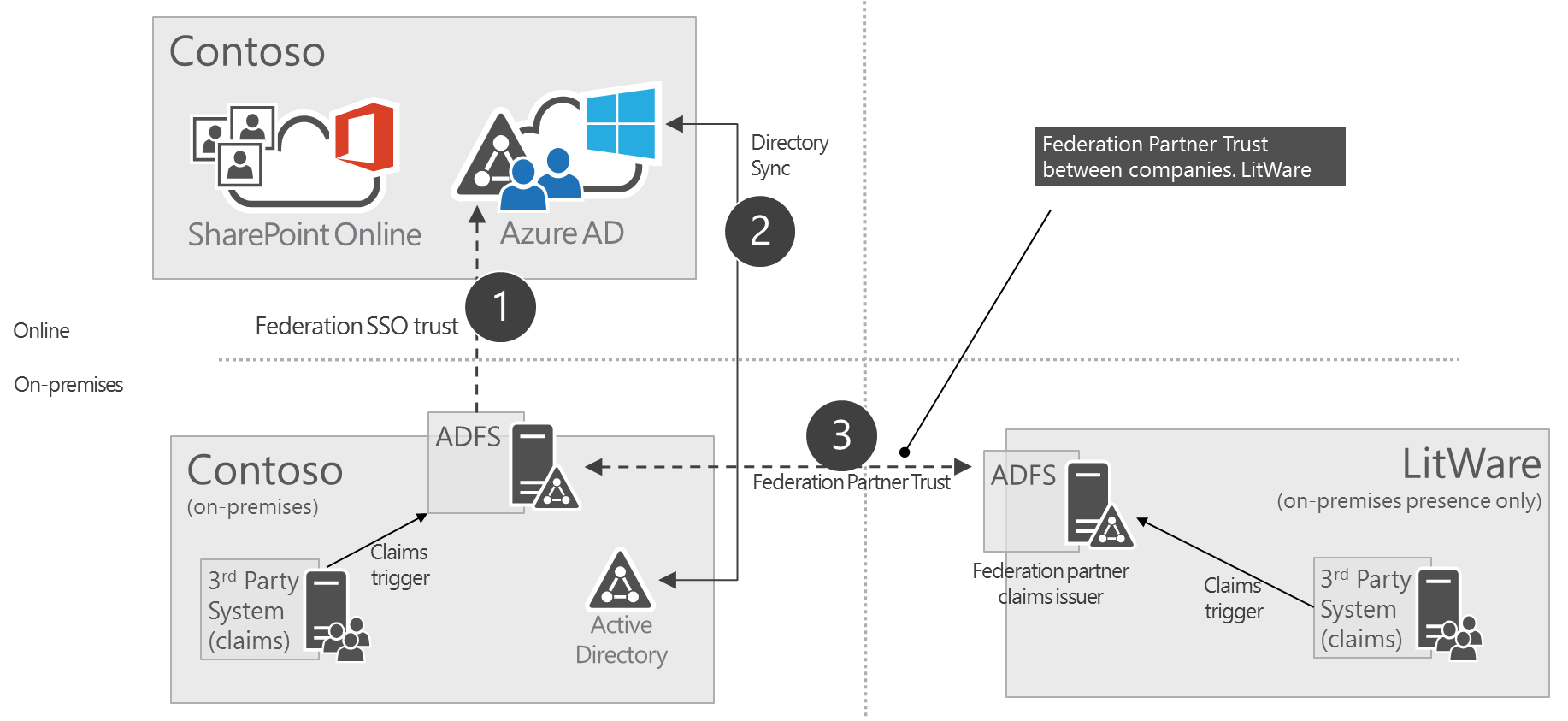
1. Normal AD connection
2. DirSync for replicating the accounts from on-premises to Azure
3. 3rd partly authorization system which contains the needed claims to be configured
4. Connection to create the needed AD groups. Could be potentially FIM or other sync tool
5. SharePoint is associated to Azure 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. Configure SharePoint online with these claims can be side and then they are exposed as resolved identities through people picker.

When users are authenticating against Office 365, they receive access to specific resources based on the claims assigned to the user. User does not need to have identity in the customer Azure AD to be able to gain access to assets.

Scenarios where this approach is applicable:

* 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

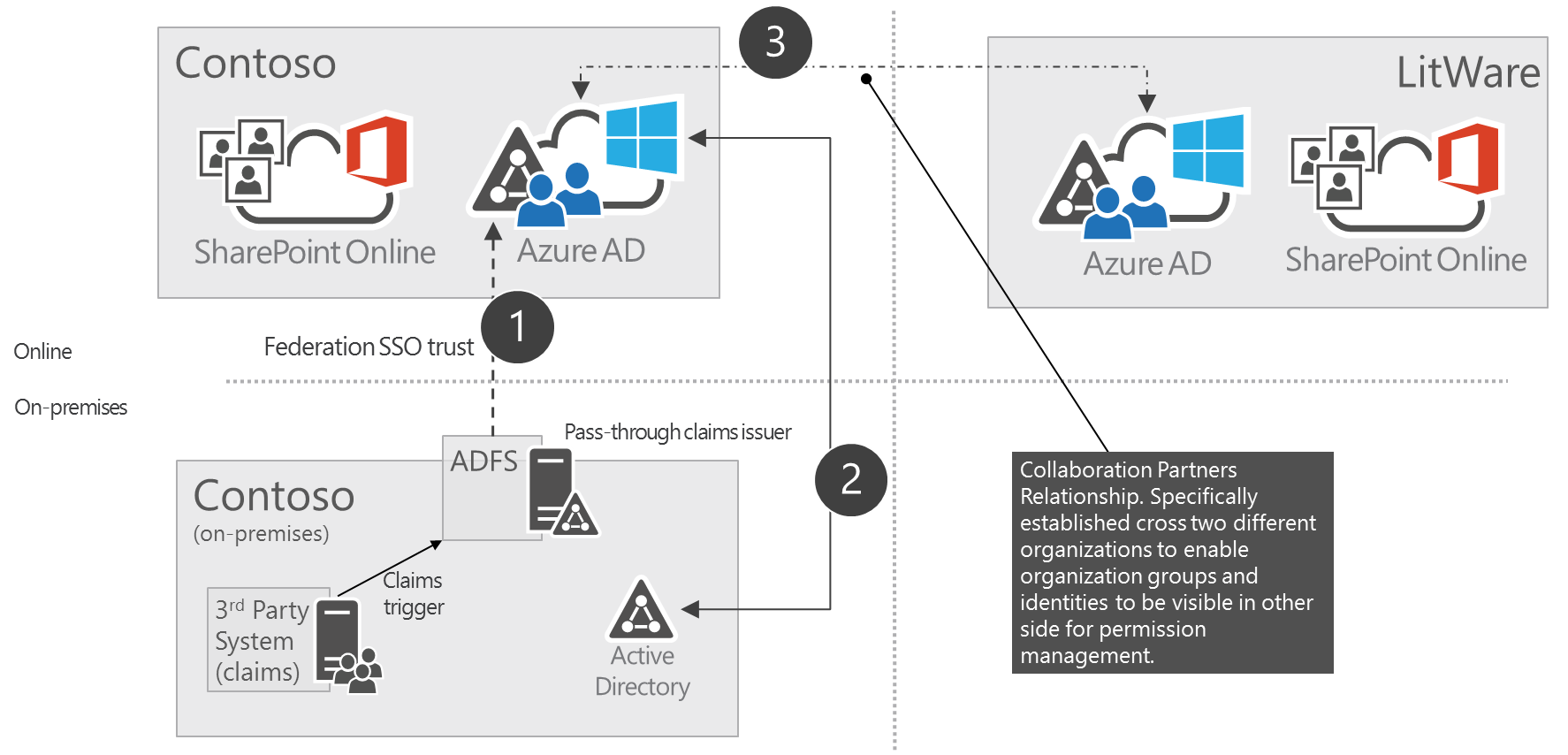


1. Normal SSO trust between on-premises and Azure
2. Identity sync’d to cloud
3. Federation partner trust to provide access on trusted accounts
   * 1. Business to business groups

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

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

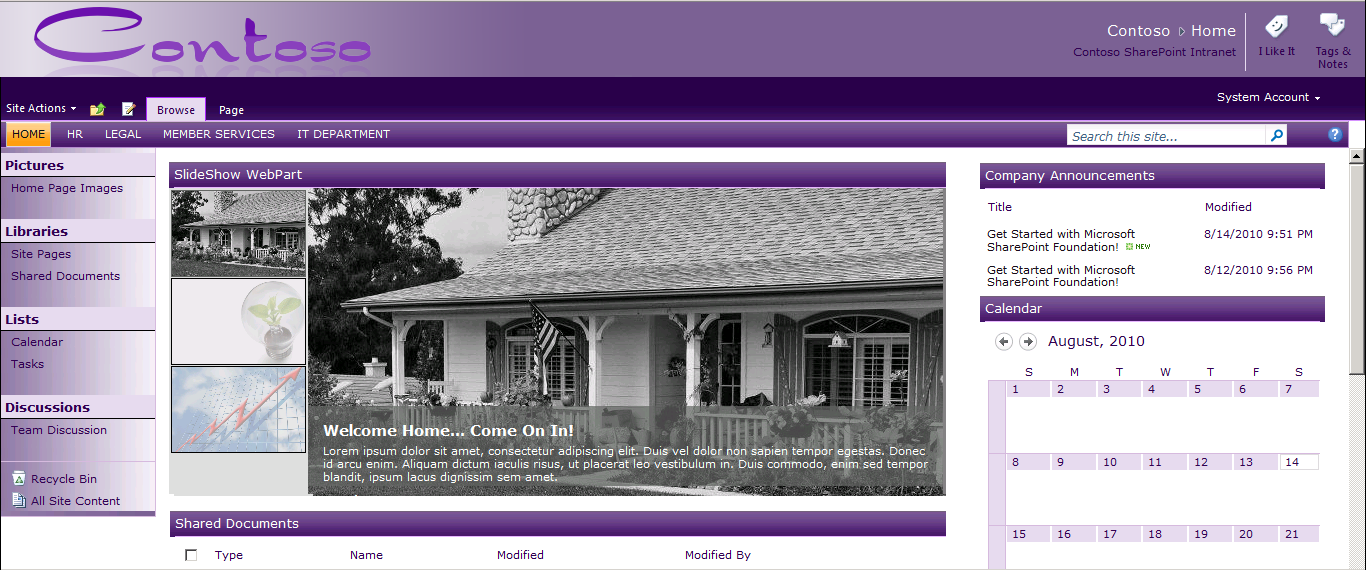


1. SSO trust for customer users
2. AD sync to Azure AD for identity mapping
3. Actual trust established with the partner organization to set permissions directly based on the ad groups from partner AD
4. Solution transformation plan
   1. Branding

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

Provides consistent branding using custom master page, applied in each site type at creation. Currently implemented using feature stapling technique in farm scope. Office 365 does not allow this.

The following picture shows the branding applied to normal team site.



To align with Office 365 recommendations this implementation will be re-developed for the Office 365 platform. This means that the branding will not be applied using custom master page. This will avoid issues with future updates that affect 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.

The branding implementation will use the 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

The following picture shows the specific UI level configurations applied using JS injection technique.

As part of this redesign, to avoid issues with constantly evolving suite navigation the layout was changed. The actual design is not yet final, but the top header navigation elements and suite navigation area are separate elements and are not to be nested. This is because the suite navigation area is consistent cross other Office 365 services.

Using the SP Color Tool create a custom spcolor (also called theme) file. A new Composed Look will have a reference to the Oslo masterpage and the new spcolor file created above. The theme will set the colors for the majority of the page elements. An alternate CSS file makes the final tweaks to the alignment of controls.

A provider-hosted app uploads these artefacts to SharePoint using a 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. The tenant administration site of the Office 365 tenant provides central control of the color
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

Customizations using JS injection technique attach 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, while in the end the page still contains required elements. It is also important to pay attention on proper client side caching to minimize any delays for showing the needed elements in the page.

The app model approach will create publishing pages with webparts. To provision Publishing Page your app requires the Write permission on the Web to create the page. Additionally, when the app is to create pages in a sub-web, it will also need the Read permission on the Site Collection in order for it to retrieve the required Page Layout to create the page.

Provisioning preconfigured Web Parts to pages is possible using the App Model.

The app creates preconfigured webparts from XML markup and adds them provisioned page using the CSOM techniques.

Replace custom list definitions with out of box list templates then perform additional configuration on the list to reach the desired state. Then use a migration tool to copy data over to the new list.

* 1. Legacy Component

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

These solutions are not in use currently. The administrator will remove them 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. The Safety List of the respective department site has the incident recorded into it. Every site has the safety news displayed on the homepage through a custom safety web part.

In addition to showing the safety incidents for the unit/department, an editor can configure the webpart to show a rolled up view of safety incidents logged in other departments.

Contoso would like to have a capability of sharing relevant news items with other colleagues something that they cannot do presently.

To achieve this using native Office 365 capabilities Contoso are changing the design of this functionality completely. Instead of tracking the news items on every site, users will create the news articles on Yammer. Every unit and department is going to have a Yammer group of its own. Postings related to safety will use the #safety tag.

The site homepage will contain the personalized Yammer feed of every user via embedded Yammer code.

User can subscribe to departments of interest. He can search for safety related news using #safety in the search bar.

Given the importance of safety at Contoso, Yammer group admins will create announcements for major safety incidents. Yammer sends email notifications for each announcement.

Mobile users can view the safety news using the Yammer mobile app without any additional customization or effort.

Users can build conversations around the safety news posting and share the safety articles with other colleagues using Yammer’s sharing feature

* 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.

Contoso can implement the same using the App model techniques.

Remote provisioning uses a 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.

By leveraging the new app model, Contoso can customize the provision process in SharePoint Online to activate specific features, capabilities, and branding to their sites.  Users complete a custom form to make a site creation request.

Contoso will prevent users from creating site collection from the browser by overriding the link to create a site collection with a link that points to a Provider-hosted app. CSOM code running in a Provider-hosted app will provision the site collection. Contoso will use a **Custom Action** using a **ScriptBlock** or **ScriptLink** to achieve redirection.

|  |  |
| --- | --- |
|  | **Additional Information** |
| *Following blog post shows a recommended technique for 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) | |

Contoso will use similar app model provisioning techniques to deploy the custom theme (spcolor file) and alternate stylesheet to the SharePoint site.

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

Contoso will use **an Azure web job** and the CSOM API to provision Personal sites. The web job will also delete the personal sites older than one year.

* 1. Record Management

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

The custom solution comprises of a Timer job that sends automated emails when a document has reached the review date. It also triggers a workflow that deletes the documents that are over 7 years old and logs the deletion information in a SharePoint list.

Contoso can achieve all of the functionality that requires full trust code in the existing SharePoint farm on the Office 365 platform using alternative means. The following table defines the new approaches 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. |

Contoso will redevelop the SP2010 workflow for SP2013; the Information Policy timer job currently calls this workflow. This will allow Contoso to make use of the new Workflow Manager’s **Call HTTP Web Service** action. A custom web service will encapsulate the required business logic. SharePoint workflow will then be invoke the web service from calls within the SharePoint workflow. A trusted service account will be required because there would be no concept of “Elevated Privileges” in the external hosting environment.

* 1. Event Handling

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

Event handlers apply custom security settings after a site is provisioned or deleted. Event handlers also update the metadata of a document after upload. Feature receivers handle the creation of site columns and content types.

This procedural code is currently loaded from a .NET assembly loaded from Global Assembly Cache (GAC) on the SharePoint server. Contoso will relocate this code to a remote hosting location, and refactor it into a **Remote Event Receiver.** In order be CAM compatible this code will use 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** perform additional provisioning or setup/cleanup on the current site collection or web up feature is activation or deactivation. For example, creating groups or adding the Content Editor Web Part to the NewForm.aspx or EditForm.aspx on the Request list. An **App Event Receiver** included in a **Provider Hosted App** will fulfill a similar provisioning role when using the Cloud App Model**.**

Custom code in Provider Hosted Apps can handle three categories of events in provider-hosted apps:

• List events, such as the adding or deleting of a list on a website.

• List item events, such as the editing of an item in a list.

• App events, such as the installation of an 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. The solution queries a SharePoint list for the required location information. The list also has sales data pertaining to the location. The solution uses Bing map API to display a map next to the locations.

SharePoint search and display templates will provide the same functionality. In the Cloud App Model approach, an app uses provisioning techniques described above to upload the display templates to Office 365.

The display template will leverage one of the existing Content Search display templates and update the managed properties accordingly.

The resulting search results page will look quite similar to the existing page.

* 1. Skill Finder

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

Allow users to search experts based on their years of experience and past projects. The solution also provides SharePoint social features that allow users to interact with the experts.

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.

In the Cloud App Model approach, an app uses provisioning techniques described above to upload the display templates to Office 365. The current look and feel will be retained using custom stylesheets.

* 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 does not require an installation on the SharePoint servers. Instead, Contoso will install it on a client machine from where it uses the SharePoint web services for content migration. It also allows operational and administrative capabilities.

The Contoso IT team have evaluated the tool and it seems to possess the same capabilities without any obvious performance impacts.

* 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. An editor will use a script editor webpart to place the JavaScript on the page.

In the Cloud App Model approach, an app uses provisioning techniques described above to upload the JavaScript to Office 365.

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**
  + Contoso will use one solution to deliver site collection and sub site creation in consistent way. Individual projects will provide different configurations and assets to for application 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**
  + Provide guidance on how to deploy required branding and other assets to the sites. Define placement and maintenance plans for content.
  + Process and tooling for handling updates on the branding elements across existing sites.
* **Development Framework**
  + Provide guidance on the hosting platform usage. This should address different 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 and then deactivate the feature responsible for the deployment. |
| List Definition | Data from existing lists will have to be migrated to out of the box list. Customize the new list 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 that 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 site creation.  Convert individual features and their element files one by one. Follow the specific guidance for feature framework elements. |
| Workflow | It is not possible to convert custom SP2010 workflows to the 2013 format. Instead, re-create each workflow in new format. Before retracting the custom workflow code from the farm stop or delete all existing running instances of the workflow. |
| 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 | Convert to remote timer job format. Delete all existing instances of the custom timer jobs before removing the full trust code from the farm. |
| Event Receivers | Convert to either remote event receivers or workflow logic. If the custom code execution does not have to be instant, remote timer job may be a solution.  Pursue alternative ways to achieve the needed result, since remote event receivers are not as reliable as the server side event receivers are. |
| Custom Features | Explicitly deactivate all custom features in the existing sites before retracting full trust solutions from the farm. |