

Enterprise Identity Management for SaaS Applications

Colin Bower

Principal Consultant - ObjectSharp

@colinbowern

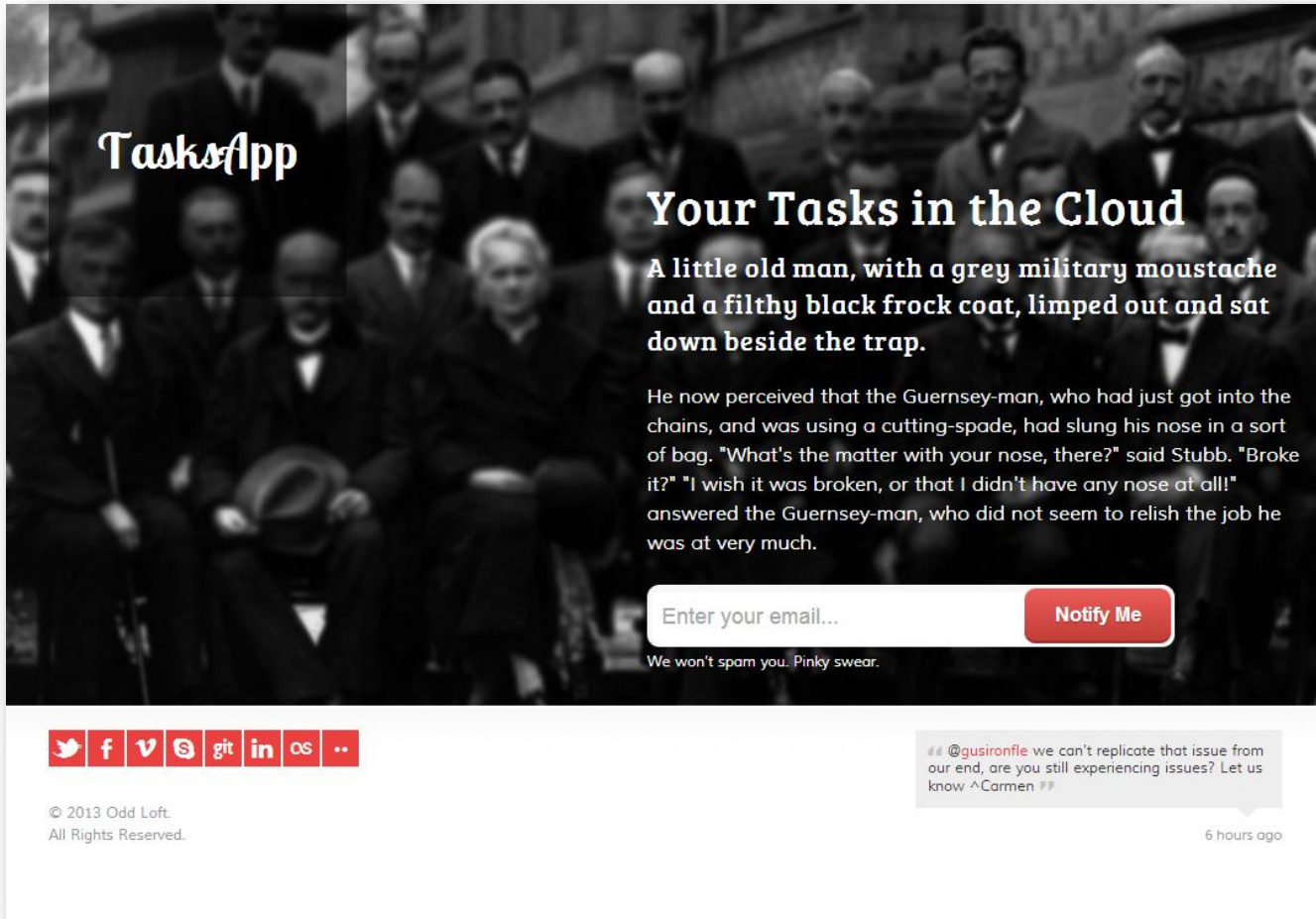
www.colinbowern.com



in this session...

- Understand how to play nice with corporate IT when you are ready to move beyond shadow IT
- Techniques to integrate with existing corporate identity systems
- How to move beyond federated identity to take advantage of the enterprise social graph

you've launched your app



TasksApp

Your Tasks in the Cloud

A little old man, with a grey military moustache and a filthy black frock coat, limped out and sat down beside the trap.

He now perceived that the Guernsey-man, who had just got into the chains, and was using a cutting-spade, had slung his nose in a sort of bag. "What's the matter with your nose, there?" said Stubb. "Broke it?" "I wish it was broken, or that I didn't have any nose at all!" answered the Guernsey-man, who did not seem to relish the job he was at very much.

Enter your email... [Notify Me](#)

We won't spam you. Pinky swear.

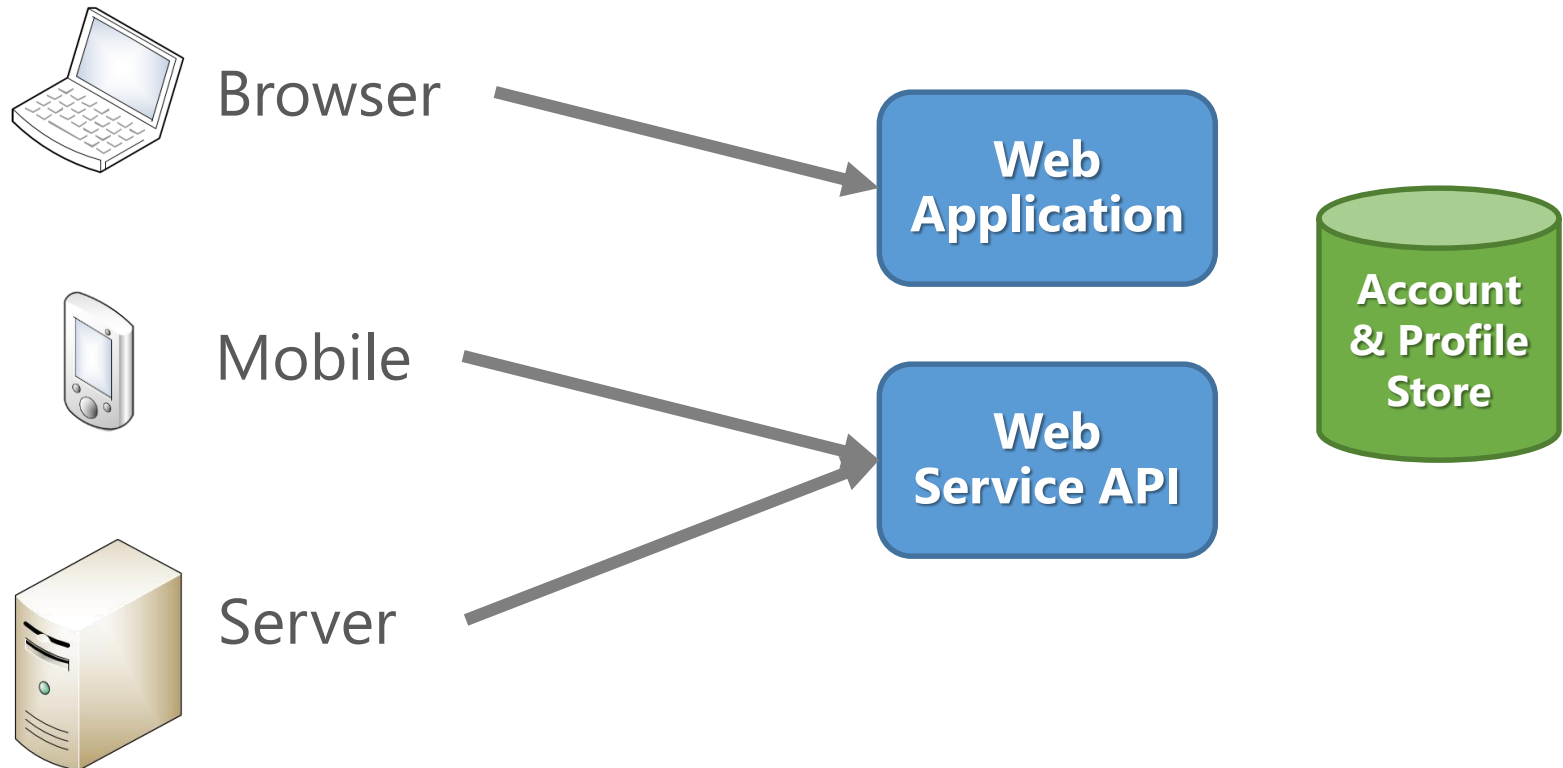
© 2013 Odd Loft.
All Rights Reserved.

6 hours ago

“ @gusironfle we can't replicate that issue from our end, are you still experiencing issues? Let us know ^Carmen ”

Twitter Facebook Vimeo SoundCloud GitHub LinkedIn OS ..

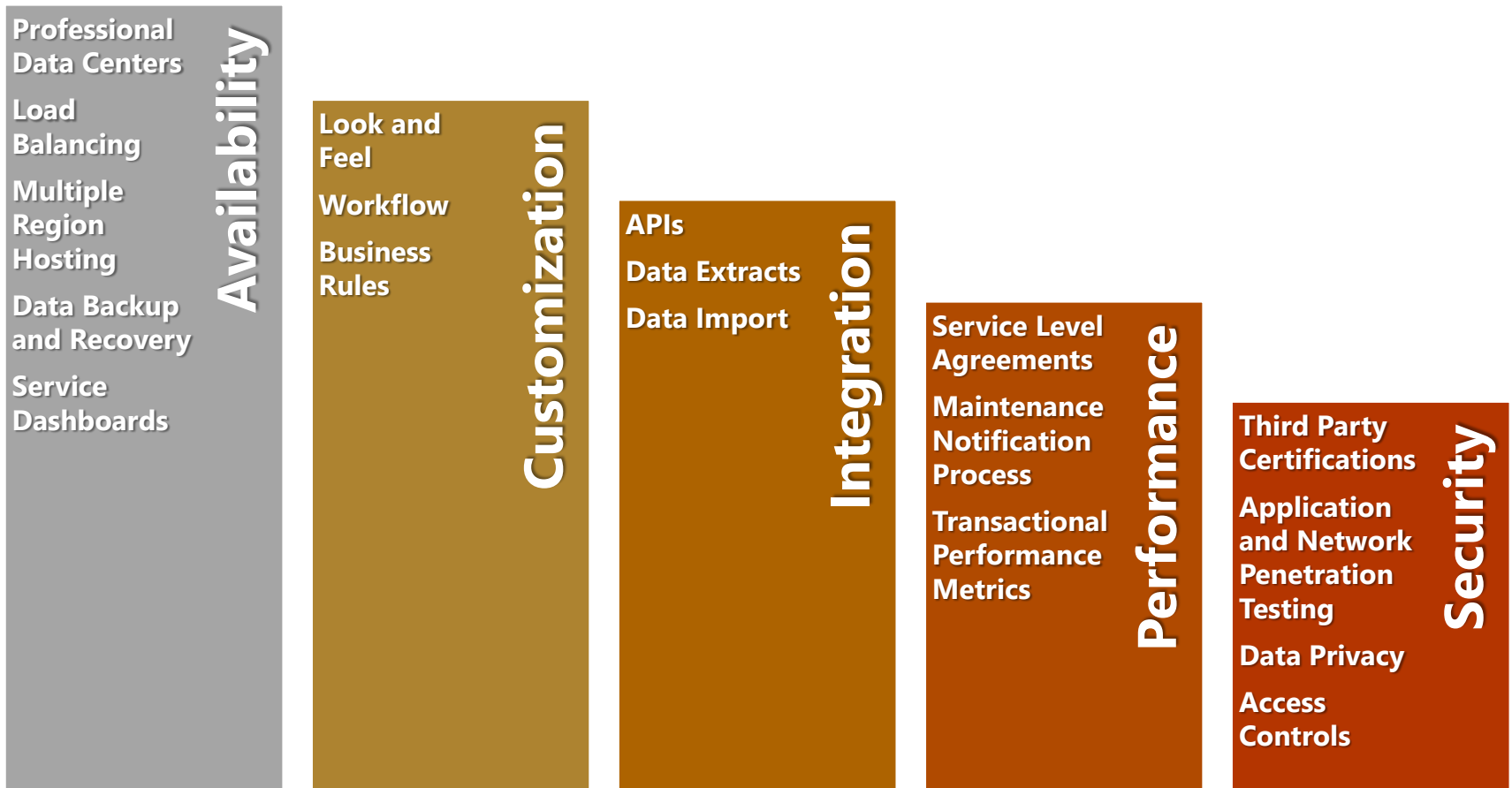
it probably looks like this



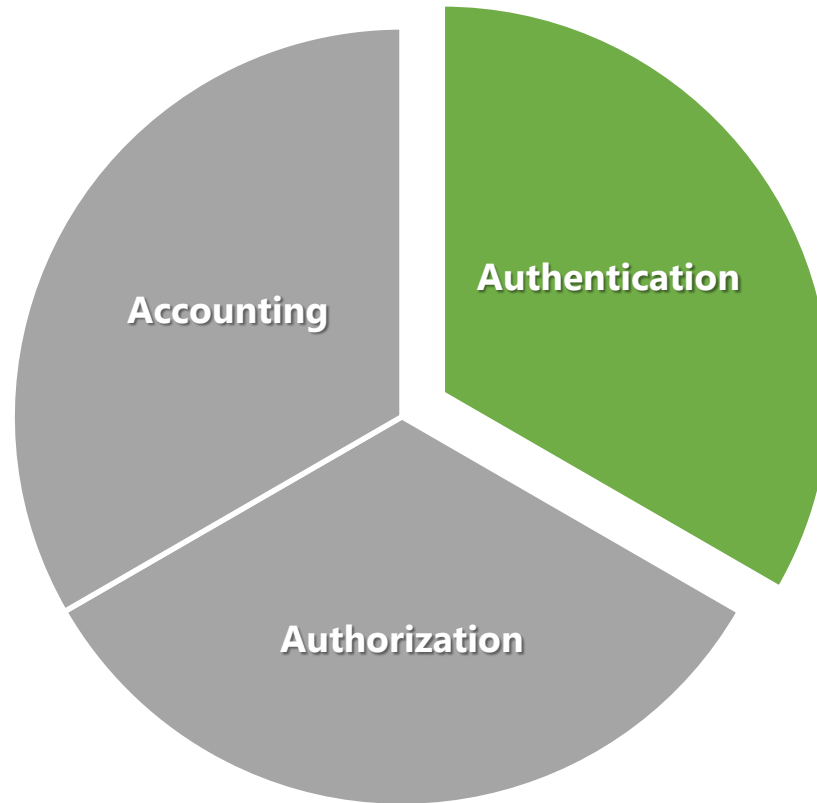
you used the common identity providers

- Local Identity
 - Username and Password
- Social Identity
 - Facebook
 - Google
 - Microsoft
 - Twitter

now go big (corporate) by offering...



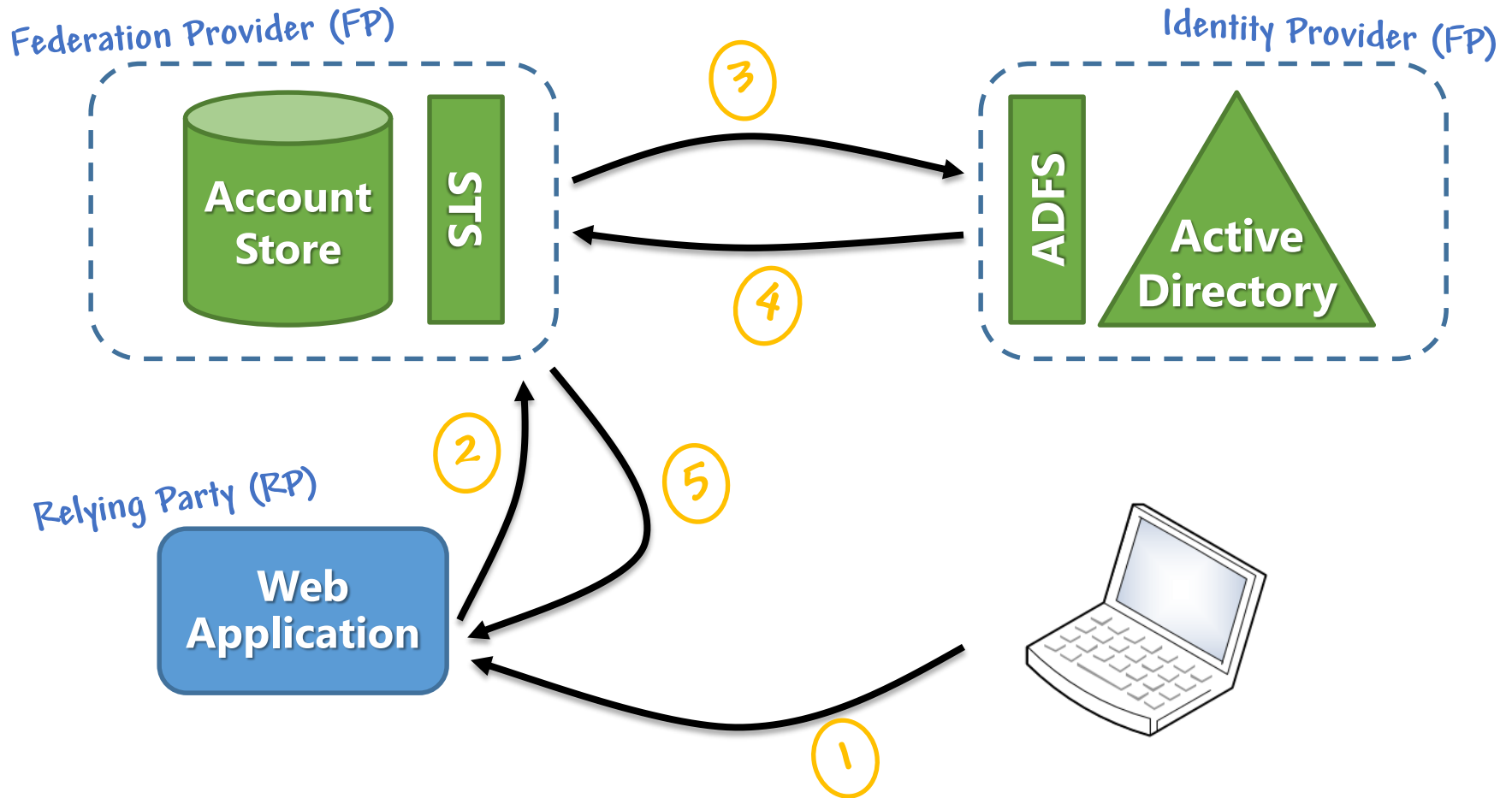
digging into enterprise class access control



corporate IT wants to know...

- What type of identity management solution is provided?
- Is Single Sign-On (SSO) provided, if so what types of SSO options are available (SAML, WS-Trust, OAuth)?
- Can your app be integrated with an existing Identity Management system?
- What type of user store is available and can it be integrated with Active Directory?
- What type of user security, authentication and authorization options are available?

...if you offer federated identity



powered by widely used standards

- Web Services Federation (WS-Federation)
 - Building on WS-* suite to enable relying parties and security token service to negotiate security tokens
 - WS-Security, WS-Trust, WS-MetadataExchange, ...
- Security Assertion Markup Language (SAML) Tokens
 - XML format for security tokens which contain user information (claims) and other relevant security-related data (signatures, token issuer)
 - SAML 2.0 extends beyond tokens to provide a protocol (SAML-P) with functionality similar to WS-Federation
- ⌚ Watch for Open ID Connect to simplify federation
 - Built on OAuth 2 with JSON/REST-based interfaces

need help explaining identity?

Identity 2.0

colinb.me/Identity20

DEMO

FEDERATED IDENTITY

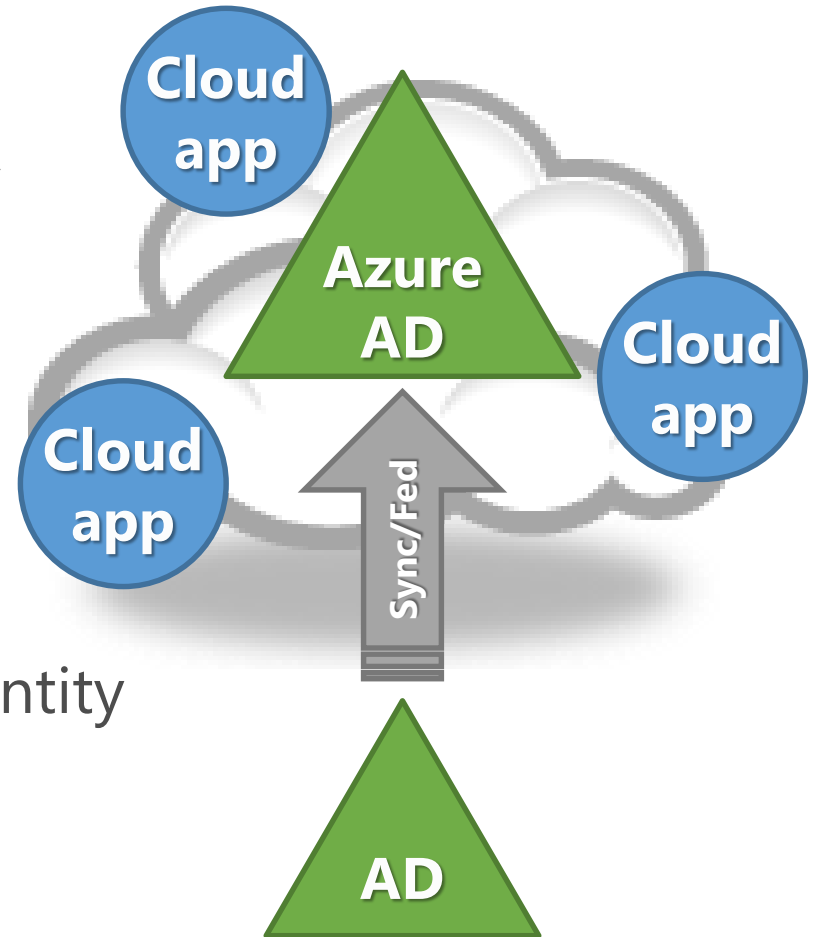
not all scenarios addressed by federation

- user provisioning / de-provisioning
- ability to view “all users” in my organization
- delegated administration

While enterprises working to consolidate identity management on premise, cloud apps are fragmenting identity... again

extending directory access to apps

- Enables federated identity and extends access to rich directory information
- Apps can read and/or write to the directory via role-based access controls
- Integrates cloud-based app identity without exposing on premise infrastructure



from a business perspective

- Enterprises extend existing AD to support cloud apps
 - Manage users, groups in AD, changes synchronized to Azure AD
 - On-premises applications use AD
 - Cloud applications use Azure AD
- Smaller businesses use Azure AD as primary identity system
 - No on-premises applications or AD
 - Use Azure AD to manage users, groups
 - Cloud application use Azure AD

under the covers Azure AD provides

- Federation provider for cloud-based applications
 - Based on Windows Azure Access Control Services
- Directory Graph API for access to directory data
 - Think LDAP, but at internet scale with REST-based API
 - Provide applications with read-only or read/write capabilities
- Broad protocol support
 - WS-Federation, SAML-P, OAuth2, Open ID Connect (future)

enables developer opportunities

- Connect with customers who have Azure AD
 - Single sign on integration instead of separate username/password
 - Query directory graph for user information, provisioning
- Use Azure AD as primary app identity system
 - Use Azure AD as local account store
 - Connect with customers using popular web identities
 - Connect with customers who have Azure AD

DEMO

DIRECTORY ACCESS

protocols used by Azure AD

Protocol	Purpose	Details
REST/HTTP	CRUD operations on directory objects, relationships	OData 3.0 compatible OAuth 2.0 authentication
OAuth 2.0	Service authentication Delegated access	JWT Token Format
Open ID Connect [†]	Web application authentication Rich client authentication	JWT Token Format
SAML 2.0	Web application authentication	SAML 2.0 Token Format
WS-Federation 1.3	Web application authentication	JWT SAML 1.1, SAML 2.0 Token Formats

[†]Currently under investigation for future release

resources

- Understanding WIF 4.5
 - colinb.me/UnderstandWIF45
- Windows Azure Active Directory
 - colinb.me/AzureAD
- Identity Server
 - thinktecture.github.io
- Vittorio Bertocci
 - cloudidentity.com
- Dominick Baier
 - leastprivilege.com
- Open ID Connect
 - openid.net/connect