ADFSToolkit

Chris Phillips, Technical Architect, CAF | InCommon-TAC| April 11 2018

Why Do This?

- Frequently asked for solution
  - I already have this installed in production, can I use it?
- Technical capabilities to install and sustaining recommended tools hard to get and keep
- At odds with technical roadmap at institution otherwise

Is it in Our Wheelhouse?

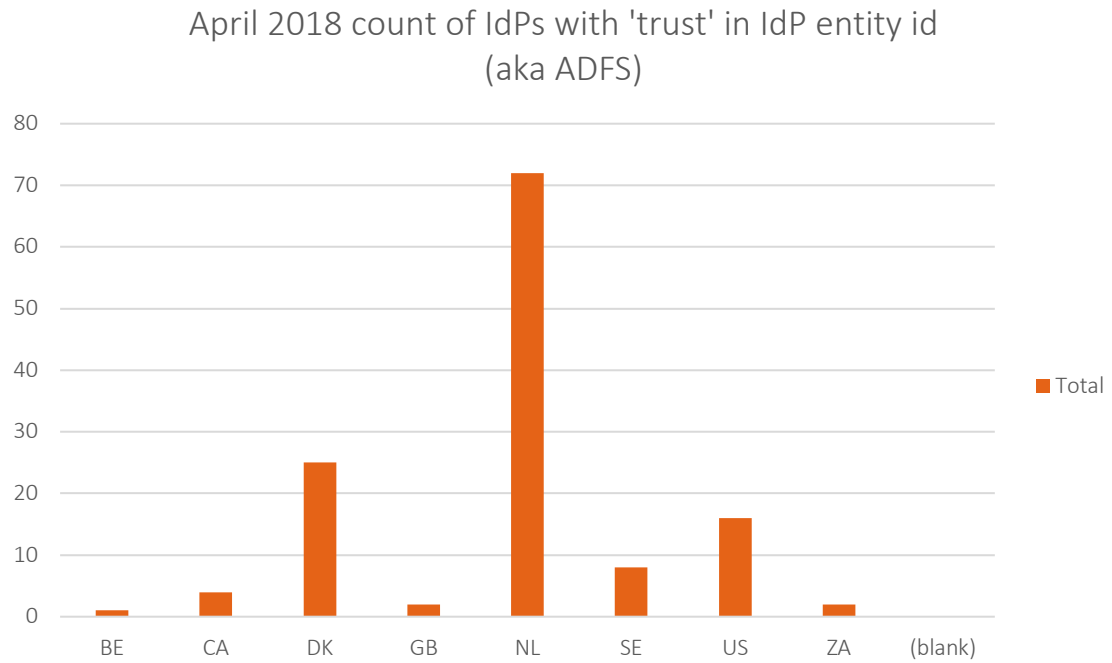
> Working on this problem aligns & helps realize our mission

- Vision
  - Research, collaboration and innovation. Anytime.
- Mission
  - CANARIE designs and delivers digital infrastructure, and drives its adoption for research, education and innovation.
- Core Purpose
  - Advancement of Canada's knowledge and innovation infrastructure.

Who is doing ADFS in R&E?

> eduGAIN: 131 live IdPs (rough search for ‘trust’)

- InCommon: 470 IdPs, 16 sites ADFS,and only 3 are green.
- CAF: 4 sites, running ADFSToolkit, 3 are green, 1 yellow



> Pace of change is changing pace:

- SWAMID is expecting upwards of 30% of IdPs in the next 12-18 months to be ADFS based.

Deployment Stats Tell Us Something..

> Q: Why focus on this if it's not a prominent platform?

```
htom:md-summary nick$ ./md-summary edugain-metadata.xml
Identity Providers (2237):
  Shibboleth              1952 ( 87.3%)
  SimpleSAMLphp            139 (  6.2%)
  OpenAthens                61 (  2.7%)
  Other                     32 (  1.4%)
  ADFS                      28 (  1.3%)
  PingFederate              14 (  0.6%)
  Authentic 2                4 (  0.2%)
  Novell Access Manager      3 (  0.1%)
  CA SiteMinder              2 (  0.1%)
  IBM Tivoli FIM             2 (  0.1%)
```

> Observation:

- It's not a prominent for a reason and has a conundrum:
  - If R&E is heavily using O365 and cloud, why are these tools NOT being re-used/dual purposed more than they are?

> Interpretation:

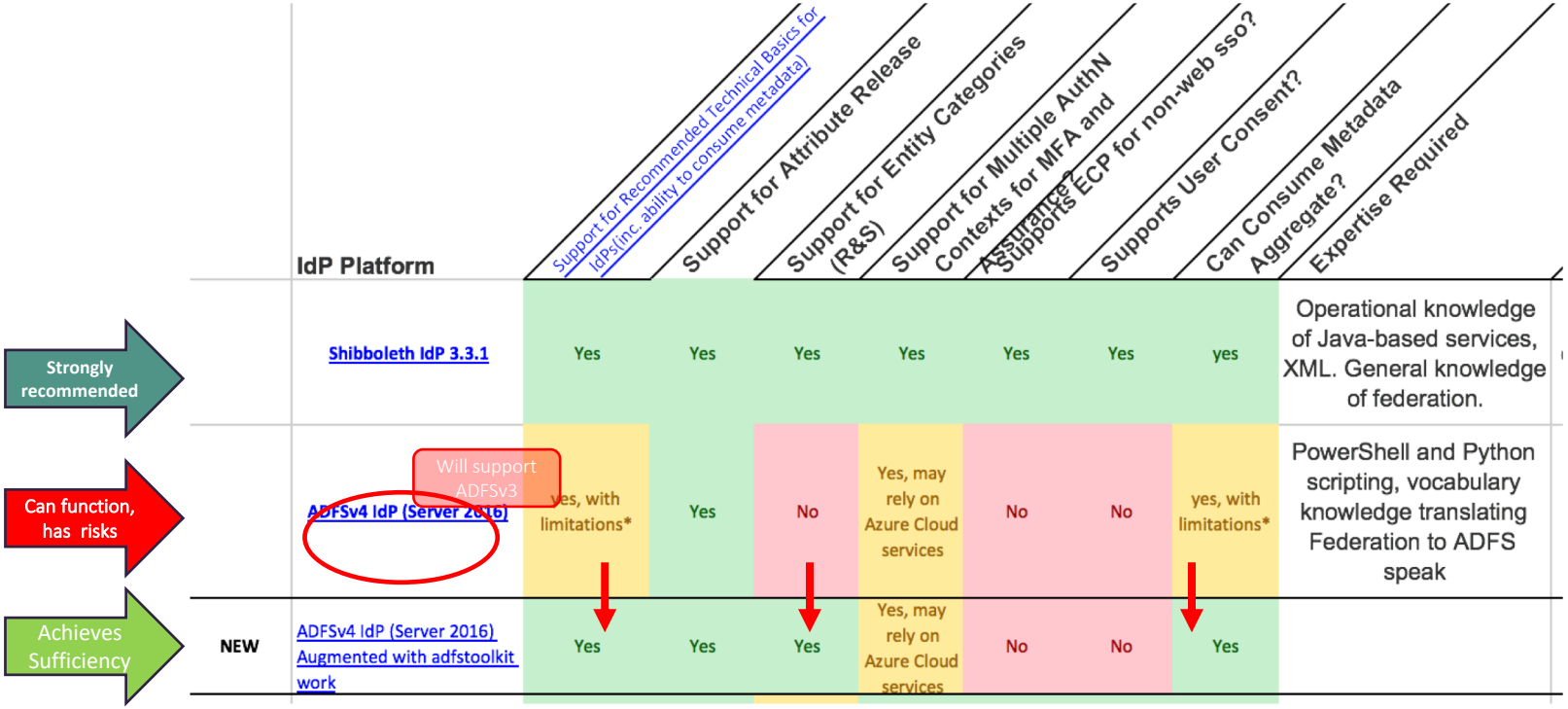
- It's what's absent that is telling
  - Despite ADFS being omnipresent, it is under utilized as an IdP - why isn't ADFS #3 or #4?
- Opportunity to invest in bridging the gap
- Not replacement to Shib. It expands federation reach to the can't and won't do it.
- Serves the underserved and self sidelined organizations
- Two tools are better than one (TIER and ADFS approach) & can be compelling.

The Question

Can we augment an infrastructure component like ADFS to participate in our federation to a level of sufficiency that despite being around for a decade, it has not met?

.. To this we claim yes.

Comparing Solutions



This is mostly around the aggregate, but there are other attribute mappings that happen for EACH SP.
Behavior right now:
Attribute release is per entity configuration by Powershell

Entity Categories Support:
Release by default, ePPN, cn, givenname, email
This is mapped to EACH SP entry in ADFS individually

Limitation was no signature validation and supporting multiple aggregates. ADFSToolkit incorporates validation before ADFS can see any records and is designed to allow scheduling of targeted ingestion of any aggregate

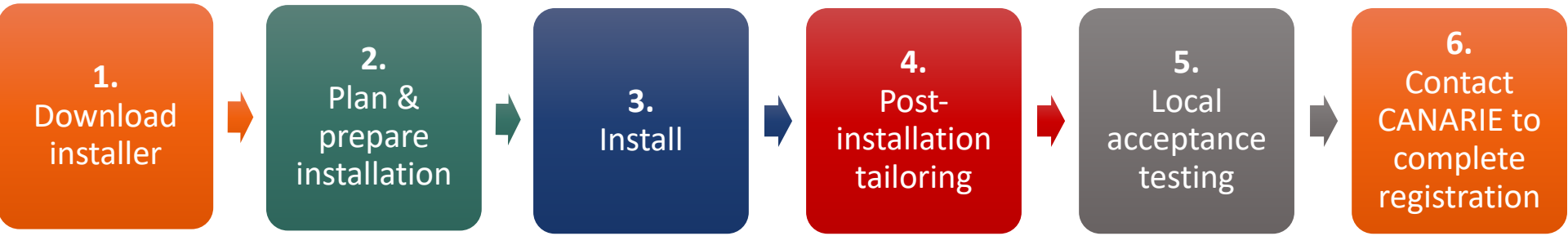
What Is ADFSToolkit?

- A toolkit that use native Powershell to augment ADFS to make R&E federation easier
- Build qualities:
  - Agnostic to federation
    - Will load any signed aggregate.
  - Has easier/more clear attribute mapping
  - Easy installation and sustainment practice
    - Uses existing Microsoft tools and lifecycle practices

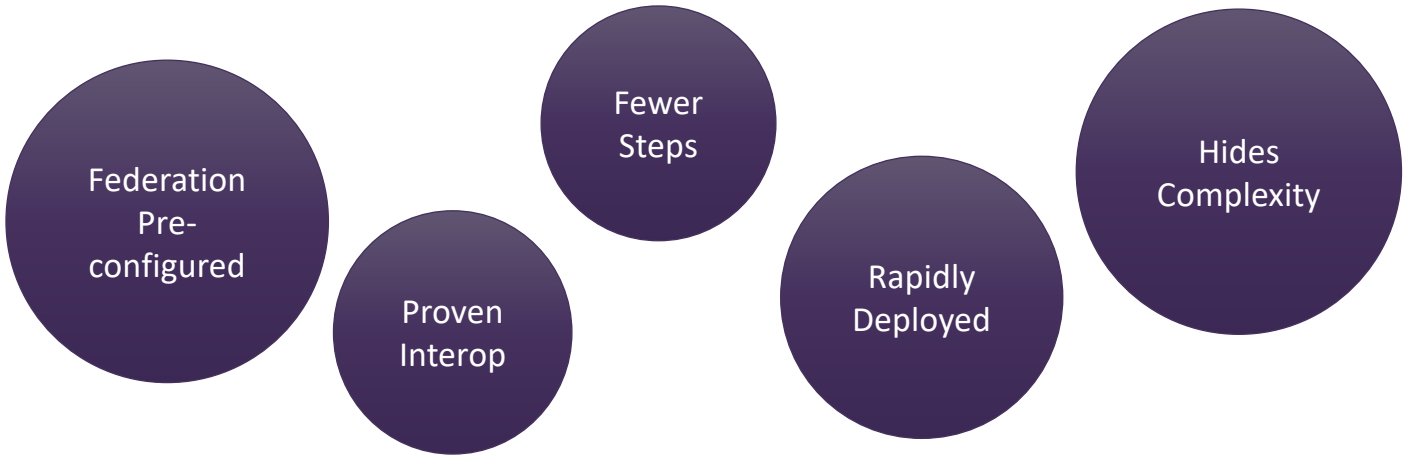
Features

- Configurable aggregate retrieval
- Signature validation by federation op key
- Ingests entities using one-at-a-time trust paradigm
- Automatic attribute release policy for R&S entity category
- Site-specific per service attribute release capability
- Sets hourly job to fetch aggregates on hourly basis
- Uses event log for easier problem diagnosis

Installation Process – Shibboleth or ADFSToolkit



> Benefits:



ADFSToolkit Software Lifecycle

Produces

Is Published

Installed by

Institution

Github.com/fedtools/adfstoolkit
- Code management
- Version Management
- Issue ingestion
- Linked documentation
- Origin for builds

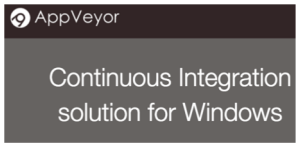
PowerShell Module
ADFSToolkit 'ADFSTk'
- One Module
- Performs all tasks
- Agnostic to organization

Published to Repository
- Easily discoverable
- Conformant to MSFT Packaging
- Official distribution technique for scripts

Sites pull from Trusted MSFT repo
- Uses built in commands
- Eases Maintenance
- Standard Practice

Is Continuously Tested

Supported by



Optional: Offers own config support
- Reference Configuration
- Hosts Extra Documentation
- First line support

Leveraged by

First time Site Install:
- Get-Command –Module PackageManager
  - Adds NuGet and PowershellGet
- Get-Command –Module ADFSToolkit
  - Fetches from <repo>
- Site reviews config
- Job is Scheduled to run hourly --> **DONE!**

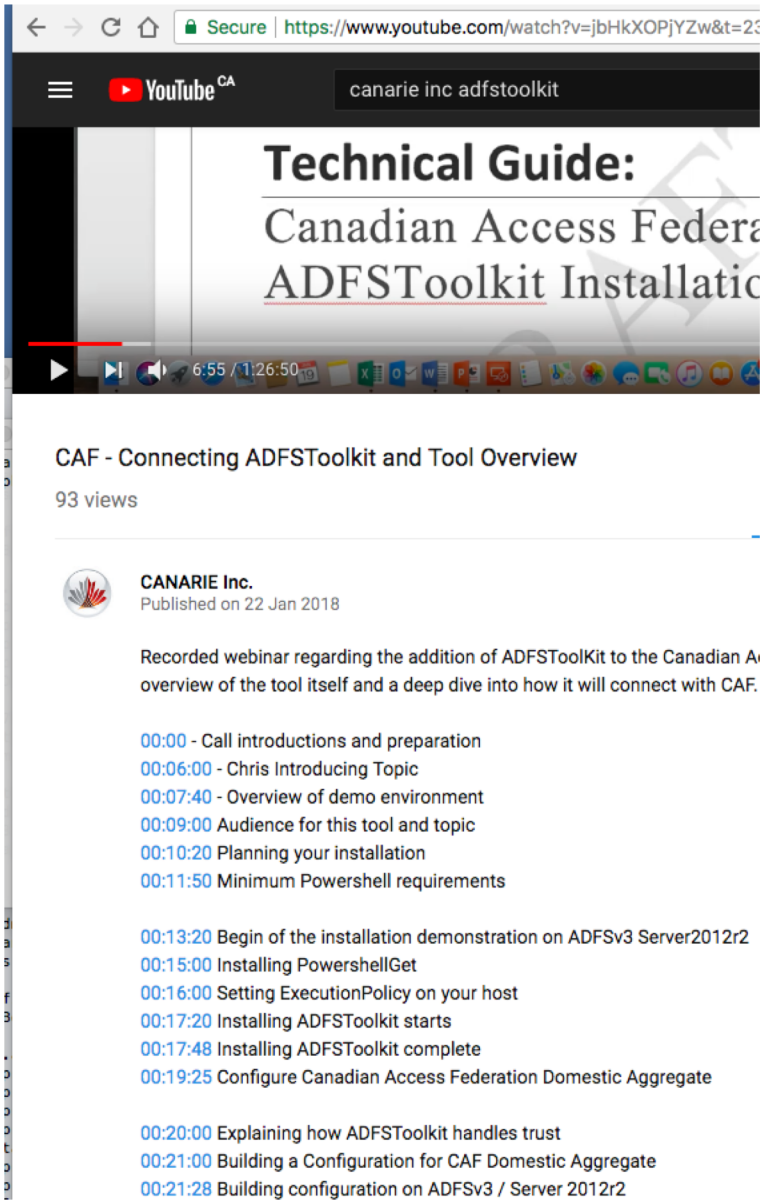
Lifecycle Maintenance Activities

Retrieving Updates:
- Manually back up work location
- Disable scheduled job
- Issue **Update-Module ADFSToolkit**
- Site reviews changes with **-WhatIf**
- Re-Enable scheduled Job

Creating Site Specific Attribute Release Policies
- **Edit get-ADFSTkLocalManualSPSettings**

Links

- Full length installation training seminar
  - https://youtu.be/jbHkXOPjYZw
  - 90 min, chaptered by function and installation step
- Link to ADFSToolkit
  - https://www.canarie.ca/identity/support/fim-tools/
- Github Issue tracker for feature requests
  - https://github.com/fedtools/adfstoolkit/issues



What's Next for ADFSToolkit Work

- 1.0 Imminent
- Reviewing early adopters feedback and taking feature requests
- 2 Workshops and presentations in Canada and presentation at TNC18

Chris' Thoughts: How can Inc-TAC serve here?

> For Keeping current and relevant to federation tech

- The more cloud admin solutions prevail, the less R&E solutions win UNLESS we weave that story into the solution
  - Deputizing ADFS to being sufficient with ADFSToolkit can be a big win
- This is also a baseline story (see stats from eduGAIN)

> You have federation peers with a solution pathway, what, if anything is absent from Best Practices in this work?

- Can US early adopters/testers/users be available? (Sweden has 2 uni's, Canada has 4 now, more weekly)
- InCommon operations could add a few things to metadata page (fingerprint) for easier use for ADFSToolkit

Chris' Thoughts: How can Inc-TAC serve here?

- Working with Microsoft has to be at all levels
  - This work is 'on the ground' and addresses an immediate need right now.
    - MSFT Server2019 could ingest our work and that would be great but still 2 years out.
  - Also working the top down approach as well
    - speak up to vendor about how ADFS could be better at all times.
- Amplifying all our R&E needs to Microsoft for both SAML, upcoming OIDC work will be important
  - how and where? What venue? (CACTI conversation?)