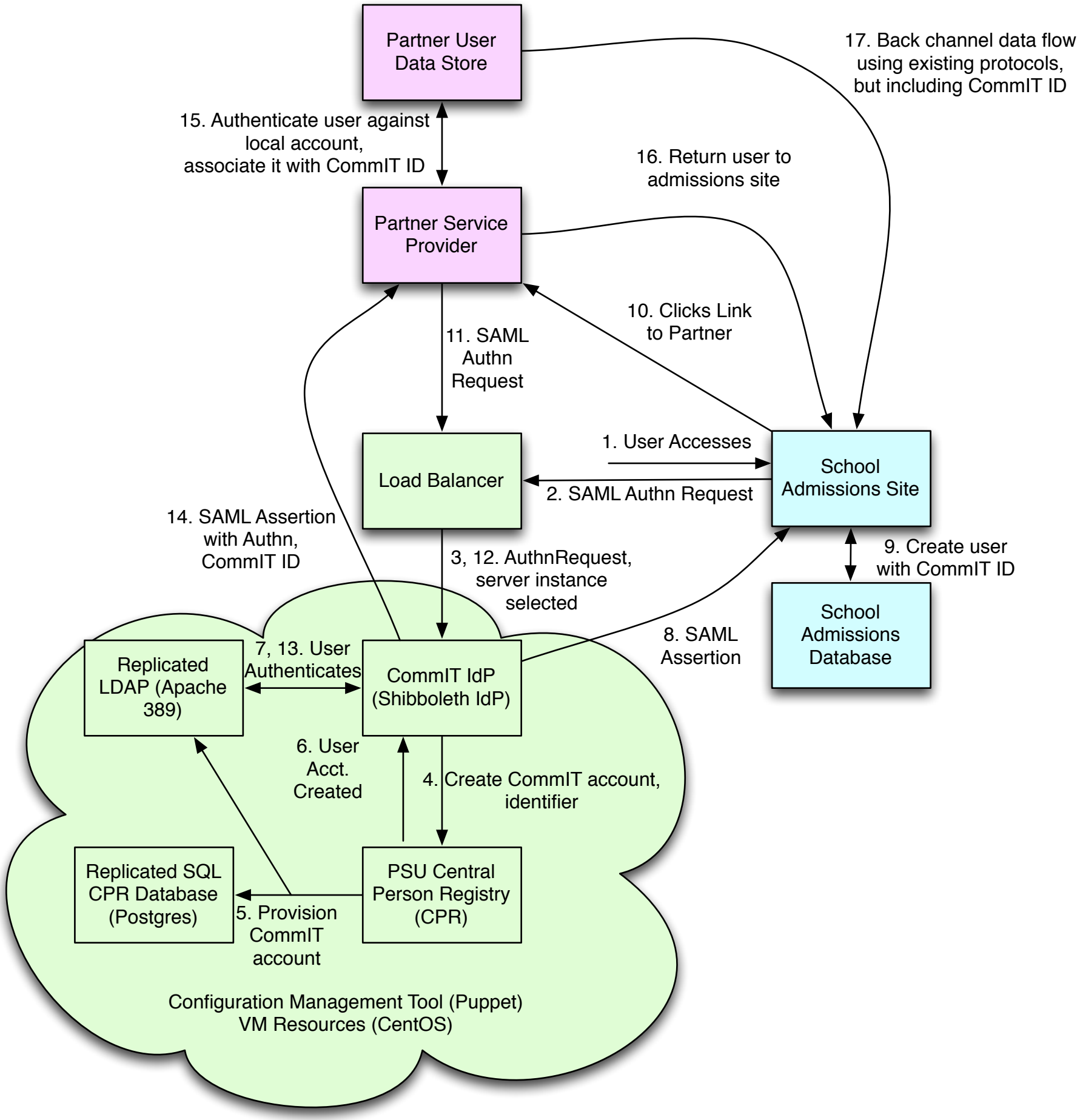
Partner User Data Store
17. Back channel data flow using existing protocols, but including CommIT ID
15. Authenticate user against local account, associate it with CommIT ID
16. Return user to admissions site
Partner Service Provider
10. Clicks Link to Partner
11. SAML Authn Request
1. User Accesses
Load Balancer
School Admissions Site
2. SAML Authn Request
14. SAML Assertion with Authn, CommIT ID
9. Create user with CommIT ID
3, 12. AuthnRequest, server instance selected
School Admissions Database
8. SAML Assertion
Replicated LDAP (Apache 389)
7, 13. User Authenticates
CommIT IdP (Shibboleth IdP)
6. User Acct. Created
4. Create CommIT account, identifier
Replicated SQL CPR Database (Postgres)
PSU Central Person Registry (CPR)
5. Provision CommIT account
Configuration Management Tool (Puppet)
VM Resources (CentOS)

1. All transactions begin with the user accessing the admissions site.
2. The admissions site redirects the user to the CommIT IdP for authentication, initiating Integration Strategy 1. IS2 could be used by the admissions site without impacting the rest of the flows.
3. The user passes through a load balancer and is associated with an IdP node.
4. The user selects, from the login interface, to create a CommIT account, presuming the user has no account yet. If the user already has an account, skip steps 4-6.
5. A CommIT account is provisioned using information supplied by the user and a CommIT identifier generated by the PSU CPR. This account is pushed out by the CPR to and stored in the PSU CPR database and the LDAP directory. Development is the responsibility of PSU, deployment the responsibility of the IdP host.
6. The user is redirected to the IdP after account creation succeeds.
7. The user is presented with the CommIT login page again and authenticates against the LDAP directory. The CommIT identifier is supplied by the directory.
8. The user is redirected by the IdP to the admissions site with a SAML assertion in hand. The assertion contains, at a minimum, information about the authentication event in an authentication statement and the CommIT identifier and a level of assurance identifier in an attribute statement.
9. A local representation of the user is created by the admissions site and used to persist the user's identity and collect data for an admissions decision.
10. Upon account creation, the user clicks a link, electing to associate admissions data with their admissions application.
11. The partner service provider, listening on a special endpoint, redirects the user to the IdP for authentication, initiating part of Integration Strategy 2. IS1 could be used by the partner service provider without impacting the rest of the flows.
12. The AuthnRequest is relayed to the same IdP that handled the initial request.
13. The user has a session with that IdP already, and SSO occurs.
14. The user is redirected by the IdP to the partner service provider site with a SAML assertion in hand. The assertion contains, at a minimum, information about the authentication event in an authentication statement and the CommIT identifier and a level of assurance identifier in an attribute statement.
15. In the context of the successful CommIT authentication and the SAML assertion, the user is authenticated against a local database holding local credentials by the partner service provider, associating the two accounts. The link is known only to the partner service provider and will be represented by storing the CommIT ID of a user as an additional field in that user's existing record.
16. The user is redirected to the admissions site and a success message is displayed.

17. Using existing protocols in the back channel, admissions data is pushed from the partner service provider to the school admissions site. The CommIT ID of the user is included in the data, allowing the admissions site to associate the admissions data with an applicant's record. A front channel flow could be implemented as part of step 16 in place of step 17.

Load balancer: association should be cookie-based, and should be active/passive. Responsibility of IdP operator(system administrator) to configure and IdP host to deploy.

VM Resources: A hosting environment containing VM's that host all CommIT infrastructure that is dynamically provisioned using the CMS. Parameters of each VM are not yet quantified but are likely to require large amounts of memory, moderate amounts of processing power, and limited amounts of data storage. Preferably geographically distributed. Number of VM's TBD based on load anticipated and load test results. Responsibility of IdP host to configure and deploy.

Configuration management system (CMS): Open-source, preferably Puppet, deploys VM's with OS, IdP, database, LDAP server, CPR. Responsibility of IdP operator(system administrator) to configure.

CommIT IdP: Open-source, preferably Shibboleth. Authenticates users against and pulls attributes from LDAP, configured with trust for all partners. Sessions not replicated; attribute queries initially unsupported, single logout never supported, replay detection never supported, artifact resolution never supported. Limited local logout supported via a cookie-clearing script. Responsibility of Internet2 and IdP operator to configure and IdP host to deploy.

Central Person Registry (CPR): An open-source person registry system that can create user accounts, provision user accounts, and reset user passwords. Responsibility of PSU CPR team to develop and configure and IdP host to deploy.

Replicated SQL CPR Database: An open-source database containing all the fields necessary for operation of the PSU CPR. All tables associated with mutable user data are replicated between all CommIT nodes. Responsibility of the database administrator and PSU CPR team to configure and IdP host to deploy.

Replicated LDAP Directory: An open-source directory containing user records provisioned by the CPR and used by the IdP as a source of authentication and attributes. All user objects are replicated between all CommIT nodes. Responsibility of the LDAP directory whiz to configure and IdP host to deploy.