

Claims

What is claimed is:

1. A computer-implemented method of authenticating clients accessing a cluster of a plurality of application hosting platform instances, the method comprising:
 - from a client authenticated to access a first application hosted on a first application hosting platform instance of the cluster via an authentication token, receiving, at a second instance of the application hosting platform, a request to access a second application hosted on the second application hosting platform instance of the cluster;
 - responsive to the request, fetching the authentication token from the client to the second instance of the application hosting platform;
 - determining one of the application hosting platform instances of the cluster as being a primary authentication application hosting platform instance;
 - sending a validation request for the authentication token to the primary authentication application hosting platform instance;
 - receiving validation confirmation of the authentication token from the primary authentication application hosting platform instance; and
 - responsive to receiving validation confirmation, granting access to the second application hosted on the second application hosting platform instance to the client.
2. One or more computer-readable media comprising computer-executable instructions that when executed cause a computing system to perform the method of claim 1.
3. The method of claim 1 wherein:
 - the validation request comprises the authentication token.
4. The method of any of claims 1 or 3 wherein:
 - the primary authentication application hosting platform instance is specified in tenant-specific configuration information; and
 - determining one of the instances of the cluster as being the primary authentication application hosting platform instance is performed using the tenant-specific configuration information.
5. The method of claim 4 wherein:
 - different primary authentication application hosting platform instances are received and stored for different tenants.

6. The method of claim 5 wherein:
receiving and storing different primary authentication application hosting platform instances
comprises receiving and storing indications of different geographical locations for the different tenants.
7. The method of any of claims 4-6 wherein:
the tenant-specific configuration information specifies on which of the plurality of platform
instances the second application is to be hosted.
8. The method of claim 7 further comprising:
redirecting requests to platform instances other than the platform instance on which the tenant-
specific configuration information specifies that the second application is to be hosted, wherein the
redirecting redirects to the platform instance on which the tenant-specific configuration information specifies
that the second application is to be hosted.
9. The method of any of claims 1 or 3-8 wherein:
fetching the authentication token from the client comprises requesting the authentication token from
client-side persistent storage.
10. The method of claim any of claims 1 or 3-9 wherein:
the request from the client is issued by an application instance having a client identifier and a client
secret;
the application instance is initially authenticated to access the first application via the client
identifier and client secret;
the application instance persists the authentication token; and
the application instance is authenticated to access the second application via the authentication
token.
11. The method of any of claims 1 or 3-10 wherein:
fetching the authentication token from the client is performed by reusing the authentication token
already stored at the client as a result of authenticating with the first application.
12. The method of claim 11 wherein:
the authentication token comprises a bearer token into which a tenant identifier has been encrypted;
the validation request sent to the primary authentication application hosting platform instance
comprises a requesting tenant identifier; and
validation fails if the requesting tenant identifier does not match the tenant identifier incorporated
into the authentication token.

13. A computing system comprising:

one or more processors;

memory;

a plurality of application hosting platform instances comprising respective platform authentication services configured to store and validate authentication tokens, one or more respective hosted applications, and tenant-specific authentication configuration information for a plurality of tenants;

wherein the platform authentication services of the application hosting platform instances are configured serve as a primary platform authentication service according to the tenant-specific authentication configuration information of a given tenant of the tenants; and

wherein the platform authentication services are configured to redirect authentication requests from the hosted applications for the given tenant to the primary platform authentication service specified for the given tenant in the tenant-specific authentication configuration information.

14. The computing system of claim 15 wherein:

a redirected authentication request comprises a request to validate an authentication token retrieved from a requesting client and is redirected from one platform authentication service to another platform authentication service for validation.