

CLAIMS

What is claimed is:

1. A computer-implemented method comprising:
in a computing system supporting a plurality of tenants accessing genomic computing services in a software-as-a-service platform that orchestrates access to genomic digital data resources via policy-based access control,
discovering a cloud provider account for an identity accessing the software-as-a-service platform;
sending a request to a credentials management service for limited temporary derived credentials valid for the cloud provider account;
receiving the limited temporary derived credentials valid for the cloud provider account;
and
providing the limited temporary derived credentials for use by the identity.
2. The computer-implemented method of claim 1 wherein:
the software-as-a-service platform supports multiple different cloud provider account types per a single tenant.
3. The computer-implemented method of any one of claims 1-2 wherein:
the software-as-a-service platform supports multiple different cloud provider accounts per a single tenant.
4. The computer-implemented method of any one of claims 1-3 further comprising:
receiving policy-based access control configuration information for the plurality of tenants;
wherein the limited temporary derived credentials are limited to rights indicated in the policy-based access control configuration information.
5. The computer-implemented method of any one of claims 1-4 further comprising:
receiving underlying credentials for the cloud provider account;
wherein the limited temporary derived credentials are derived from the underlying credentials.

6. The computer-implemented method of any one of claims 1-5 wherein:
the software-as-a-service platform supports limited temporary derived credentials for a plurality of cloud provider types.
7. The computer-implemented method of claim 6 wherein:
discovering the cloud provider account comprises discovering a cloud provider type of the cloud provider account.
8. The computer-implemented method of any one of claims 1-7 wherein:
the identity is one of a plurality of different identity types supported by the software-as-a-service platform.
9. The computer-implemented method of claim 8 wherein:
the identity is of type “application.”
10. The computer-implemented method of claim 8 wherein:
the identity is of type “workgroup.”
11. The computer-implemented method of claim 10 wherein:
a workgroup identity spans a plurality of the tenants of the software-as-a-service platform.
12. The computer-implemented method of any one of claims 8-11 wherein:
the identity types supported by the software-as-a-service platform comprise:
application;
tenant;
workgroup; and
user.
13. The method of any one of claims 1-12 wherein:
the cloud provider account stores a genomic digital data resource;
access to the genomic digital data resource is controlled by a role identifier linked to a policy-based access control definition; and
the method further comprises:

responsive to a request for access to the genomic digital data resource, providing the role identifier specified in the policy-based access control definition for the request for access.

14. One or more computer-readable media comprising:
computer-executable instructions capable of causing a computing system to perform the method of any one of the claims 1-13.

15. A multi-tenant, cloud-based system comprising:
one or more processors;
memory coupled to the one or more processors;
a mapping between identities accessing a software-as-a-service platform and cloud provider accounts;
a policy store comprising policy-based access control definitions;
a genomic digital data resource linked to a role identifier and stored at a given cloud provider account external to the software-as-a-service platform;
wherein the memory comprises computer-executable instructions causing the one or more processors to perform operations comprising:
based on the mapping, discovering a cloud provider account for an identity accessing the software-as-a-service platform;
sending a request to a credentials management service for limited temporary derived credentials valid for the cloud provider account;
receiving the limited temporary derived credentials valid for the cloud provider account;
and
providing the limited temporary derived credentials for use by the identity to access the genomic digital data resource.

16. The system of claim 15 wherein:
the software-as-a-service platform supports multiple different cloud provider account types per tenant; and
the software-as-a-service platform supports multiple different cloud provider accounts per tenant.