CLAIMS

1. A computer-implemented method comprising:

in a computing system supporting a plurality of accessing 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, wherein the limited temporary derived credentials are based on a policy-based access control definition, the limited temporary derived credentials are limited to rights permitted in the policy-based access control definition, the limited temporary derived credentials are based on underlying credentials, and the limited temporary derived credentials provide more limited access than the underlying credentials; and

providing the limited temporary derived credentials for use by the identity;

wherein:

the limited temporary derived credentials are based on a policy-based access control definition are generated based on underlying credentials provided via cloud provider account management, the limited temporary derived credentials are valid for the cloud provider account, and the limited temporary derived credentials provide access to the genomic digital data resources;

the software-as-a-service platform is configured to support a specified cloud provider type selected from multiple different cloud provider type as specified by an administrative service;

the underlying credentials are persisted in a credentials object;

the credentials object stores the specified cloud provider type selected from the multiple different cloud provider types for the underlying credentials; and

the specified cloud provider type selected from among the multiple different cloud provider types is provided during cloud provider account discovery;

wherein:

the method further comprises storing, by the cloud provider account, a genomic digital data resource;

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.

2. The computer-implemented method of claim 1 further comprising:

supporting, by the software-as-a-service platform, multiple different cloud provider account types per a single tenant.

3. The computer-implemented method of any one of claim 1 further comprising:

support, by the software-as-a-service platform, multiple different cloud provider accounts per a single tenant.

4. The computer-implemented method of claim 1 further comprising:

receiving policy-based access control configuration information for the plurality of accessing 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 claim 1 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 claim 1 further comprising:

supporting, by the software-as-a-service platform, 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 claim 7 wherein:

the credentials management service is external to the software-as-a-service platform.

9. The computer-implemented method of claim 1 wherein:

the identity is one of a plurality of different identity types supported by the software-as-a-service platform.

10. The computer-implemented method of claim 9 wherein:

the identity is of type “application.”

11. The computer-implemented method of claim 9 wherein:

the identity is of type “workgroup.”

12. The computer-implemented method of claim 11 wherein:

spanning, by a workgroup identity, a plurality of accessing tenants of the software-as-a-service platform, wherein the workgroup identity provides cross-tenant access to cloud provider accounts.

13. The computer-implemented method of claim 9 wherein:

the identity types supported by the software-as-a-service platform comprise:

application;

tenant;

workgroup; and

user.

14. A computing system supporting a plurality of accessing tenants accessing genomic computing services in a soft-as-a service platform that orchestrates access control, wherein the computer system comprises: one or more processors;

memory coupled to the one or more processors;

wherein the memory comprises computer-executable instructions causing the one or more processors to perform operations comprising:

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, wherein the limited temporary derived credentials are based on a policy-based access control definition, the limited temporary derived credentials are limited to rights permitted in the policy-based access control definition, the limited temporary derived credentials are based on underlying credentials, and the limited temporary derived credentials provide more limited access than the underlying credentials; and

providing the limited temporary derived credentials for use by the identity;

wherein:

the limited temporary derived credentials are based the policy-based access control definition are generated based on underlying credentials provided via cloud provider account management, the limited temporary derived credentials are valid for the cloud provider account, and the limited temporary derived credentials provide access to the genomic digital data resources;

the software-as-a-service platform is configured to support a specified cloud provider type selected from multiple different cloud provider types as specified by an administrative service;

the underlying credentials are persisted in a credentials object;

the credentials object stores the specified cloud provider type selected from the multiple different cloud provider types for the underlying credentials; and

the specified cloud provider type is selected from among the multiple different cloud provider types is provided during cloud provider account discovery;

wherein:

the operations further comprise storing, by the cloud provider account, 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 operations further comprise:

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.

15. The system of claim 14 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.

16. The system of claim 14 wherein the memory further comprises computer-executable instructions causing the one or more processors to perform operations comprising:

granting access to the genomic digital data resource according to a policy-based access control definition evaluated at a time of a request for access.

17. The system of claim 14 wherein:

the identity is one of a plurality of different identity types supported by the software-as-a-service platform.

18. The system of claim 14 wherein:

the identity is of type “application.”

19. The system of claim 14 wherein:

the identity is of type “workgroup.”

20. The system of claim 19 wherein:

the operations further comprise:

spanning, by a workgroup identity, a plurality of the tenants of the software-as-a-service platform.

21. One or more non-transitory computer-readable storage media comprising:

computer-executable instructions capable of causing a computer system to perform the following:

in a computing system supporting a plurality of accessing tenants accessing genomic computing services in 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, wherein the limited temporary derived credentials are based on a policy-based access control definition, the limited temporary the limited temporary derived credentials are rights permitted in policy-based access control definition, the limited temporary derived credentials are based on underlying credentials, and the limited temporary derived credentials provide more limited access than the underlying credentials; and

providing the limited temporary derived credentials for use by the identity;

wherein:

the limited temporary derived credentials are based on policy-based access control definition are generated based on underlying credentials provided via cloud provider account management, the limited temporary derived credentials are valid for the cloud provider account, and the limited temporary derived credentials provide access to the genomic digital data resources;

the underlying credentials are persisted in a credentials object;

the credentials object stores the specified cloud provider type selected from the multiple different cloud provider types for the underlying credentials; and

the specified cloud provider type selected from among the multiple different cloud provider types is provided during cloud provider account discovery;

wherein:

the instructions are further capable of causing the computing system to perform storing, by the cloud provider account, 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 instructions are further capable of causing the computing system to perform:

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.