

CLAIMS

1. A method for provisioning an existing secondary identity and access management instance with a new secondary identity and access management instance, comprising:

receiving a request to provision the new secondary identity and access management instance for an existing secondary identity and access management instance;

creating a primary identity and access management instance for the existing identity and access management instance and the new secondary identity and access management instance;

aggregating data from the existing secondary identity and access management instance to the primary identity and access management instance;

deploying a request handler to the primary identity and access management instance to handle incoming requests for the identity and access management instance;

changing a reconciliation process and an audit process from the existing secondary identity and access management instance to the primary identity and access management instance thereby changing the existing secondary identity and access management instance to the new secondary identity and access management instance for the primary identity and access management instance;

deploying the new secondary identity and access management instance to the primary identity and access management instance; and

deploying at least one application to the new secondary identity and access management instance based on an operation processed by the new secondary identity and access management instance.

2. The method of claim 1, wherein the request to provision the new secondary identity and access management instance is received by the existing secondary identity and access management instance.

3. The method of claim 1, wherein the request to provision the new secondary identity and access management instance comprises an identification of a target endpoint type for the new secondary identity and access management instance.

4. The method of claim 3, wherein the target endpoint type comprises one of a mainframe, infrastructure as a service, a human, and a non-human.

5. The method of claim 1, further comprising:
verifying that hardware to support the new secondary identity and access management instance is available.

6. The method of claim 1, wherein the data aggregated from the existing secondary identity and access management instance comprises data from the existing secondary identity and access management instance's identity and access management database.

7. The method of claim 1, wherein the request handler processes requests with an access catalog.

8. The method of claim 1, wherein the step of deploying the new secondary identity and access management instance comprises updating logic the

primary identity and access management instance to recognize target endpoints for the new secondary identity and access management instance.

9 The method of claim 3, wherein the at least one application that is deployed to the second identity and access management instance is associated with the target endpoint type for the new secondary identity and access management instance.

10. A system for provisioning an existing instance with a new secondary instance, comprising:

- an existing secondary identity and access management instance;

- a primary identity and access management instance; and

- a new secondary identity and access management instance;

wherein:

- in response to receiving a request to provision the new secondary identity and access management instance for the existing secondary identity and access management instance, the primary identity and access management instance aggregates data from the existing identity and access management instance;

- the primary identity and access management instance's request handler is updated to handle incoming requests for the existing identity and access management instance;

- the primary identity and access management instances' reconciliation process and audit process are changed from the existing identity and access management instance to the primary identity and access management instance; and

at least one application is deployed to the new secondary identity and access management instance based on an operation processed by the new secondary identity and access management instance.

11. The system of claim 10, wherein the request to provision the new secondary identity and access management instance is received by the existing identity and access management instance.

12. The system of claim 10, wherein the request to provision the new secondary identity and access management instance comprises an identification of a target endpoint type for the new secondary identity and access management instance.

13. The system of claim 12, wherein the target endpoint type comprises one of a mainframe, infrastructure as a service, a human, and a non-human.

14. The system of claim 10, further comprising a host program or application that verifies that hardware to support the new secondary identity and access management instance is available.

15. The system of claim 10, wherein the data aggregated from the existing secondary identity and access management instance comprises data from the existing secondary identity and access management instance's identity and access management database.

16. The system of claim 10, wherein the request handler processes requests with an access catalog.

17. The system of claim 10, wherein logic in the primary identity and access management instance is updated to recognize target endpoints for the new secondary identity and access management instance.

18. The system of claim 12, wherein the at least one application that is deployed to the second identity and access management instance is associated with the target endpoint type for the new secondary identity and access management instance.