SERIES Number 12

INTELLIGENCE AFTER NEXT

MAKING INTEGRATION A REALITY: ENTERPRISE ICAM SERVICES WITH C2E

by Christopher Bashioum and Cheryl Clopper

22-2937 09-15-2022

Efficiently Keeping Users Connected to Cloud Data and Resources

President Biden on May 12 of 2021 signed Executive Order 14028, "Improving the Nation's Cybersecurity", directing the adoption of Zero Trust Architecture (ZTA) in Federal Agencies as they move to the cloud. The subsequent Zero Trust Maturity Model promulgated by the Cybersecurity & Infrastructure Security Agency (CISA) states that "identity will form a core component of an agency's ZTA" and that "as agencies migrate services to the cloud … [they] will need to integrate their on-premises identities with those in the cloud environments".

To maximize the ability for authorized consumers to access data, to minimize system complexity, and to reduce costs, we recommend the Intelligence Community (IC) actively encourage and incentivize programs to use enterprise Identity, Credential, and Access Management (ICAM) services for protecting government-owned resources that are deployed on the Commercial Cloud Enterprise (C2E) vendor's clouds, and actively identify and remove any disincentives for programs to use the enterprise ICAM services.

The goal should be for government-owned resources to leverage IC PKI to authenticate consumers and leverage enterprise managed Attribute Based Access Control (ABAC) attributes for authorization decisions related to the authenticated consumers. This would drive consistent cloud vendor agnostic access control policies and data tagging efforts for all government-owned resources, enabling consumers to gain access to the data they are legitimately authorized to consume.

The Cloud Vendors

The IC recently awarded the C2E contract to five cloud vendors: Amazon, Microsoft, Google, Oracle, and IBM. The contract is an Indefinite Delivery, Indefinite Quantity (IDIQ) multi-award contract wherein the five companies compete for specific task orders.

The cloud offerings for C2E include Amazon Web Services (AWS), Microsoft Azure, IBM Cloud, Google Cloud, and Oracle Cloud. Each cloud vendor will provide ICAM services as part of the core cloud functionality available on each of the network domains. They include:

- **Identity Management** – managing digital identities and their associated authorization attributes for both person entities (PEs) and non-person entities (NPEs).
- **Credential Management** – managing credentials and their associated authenticators used to authenticate PEs and NPEs attempting to access a protected resource.
- **Access Management –** particularly the authentication and authorization mechanisms that leverage trusted identifies and authoritative credentials to ensure only permitted PEs and NPEs are granted access to protected resources.[1]

While each of the cloud vendors provide ICAM services for tenants of their clouds, the implementations of these ICAM services differ in vocabulary, user interfaces, Application Programming Interfaces (API), Software Development Kits (SDK), authenticators supported, and authorization policies supported. In addition, each of the C2E cloud vendors provides separate ICAM solutions for the following two different classes of cloud-hosted protected resources:

- Government-owned resources (e.g., web application)
- Cloud vendor-owned resources (e.g., elastic compute, Simple Storage Service (S3) bucket)

As the government begins to deploy data to the clouds available via C2E and implement ZTA according to the Presidential Directive, we have identified four potential ICAM-related issues associated with the adoption of C2E. They include:

- Consumers not being able to get the data they are. legitimately authorized to consume.
- Reduced enterprise security posture.
- Increased costs to the government.
- Misalignment with stated enterprise architecture goals.

Cloud Vendor-Provided ICAM Services

All the cloud vendors provide services to manage identities, attributes, and credentials local to the cloud vendor and support federation of identities, attributes, and credentials managed by an external identity provider (IdP) via Security Assertion Markup Language (SAML). The cloud vendors' authentication, authorization, and attribute services can be used to protect government-owned resources deployed on their cloud offerings by integrating with the government-owned resources via SAML and OpenID Connect (OIDC), and in some cases via SDKs written for node.js and/or Java and in other cases via well-defined APIs.

The documentation for each of the cloud vendors' ICAM services can be somewhat confusing as to which class of protected resource their ICAM services are intended to protect.

The documentation tends to conflate using the cloud vendors' ICAM services for protecting the cloud vendor-owned resources that are managed by a given tenant (i.e., a program) with protecting the government-owned resources that are deployed by the tenant in a vendor's cloud. In case the reader wishes to investigate each of the cloud vendor's ICAM services in more detail, the following list may provide some assistance:

- For protecting cloud vendor-owned resources:
  - AWS Commercial Cloud Services (C2S): Identity and Access Management (IAM)
  - Microsoft Azure: Azure Managed Identities
  - IBM Cloud: IBM Access Management
  - Google Cloud: IAM
  - Oracle Cloud: Oracle Cloud Infrastructure IAM
- For protecting government-owned resources deployed on the vendor's cloud:
  - AWS C2S: Amazon Cognito
  - Microsoft Azure: Application Management
  - Single Sign-On (SSO)
  - IBM Cloud: IBM App Id
  - Google Cloud: Google Cloud Identity
  - Oracle Cloud: Oracle Identity Cloud Service

Note that in each case (except for Microsoft Azure), the cloud vendor-provided ICAM services for protecting government-owned resources deployed on the vendor's cloud are less mature and less complete than the cloud vendor-provided ICAM services for protecting the cloud vendor-owned resources.

Enterprise-Provided ICAM Services

Each of the "Big 5" IC agencies - Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), National Geospatial-Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA) - provide enterprise ICAM services for protecting government-owned resources. Like the cloud vendors, the implementations of these ICAM services differ from each other in terms of user interfaces, APIs, and SDKs. Unlike the cloud vendors, the implementation of these ICAM services tend to use the same vocabulary, support the same authenticators and authorization policies, and federate identities and attributes with each other via the Unified Authorization and Attribute Service (UAAS).

All the IC enterprise ICAM services manage identities, attributes, and credentials at the enterprise level. They generally get the authoritative identity and attribute information from the applicable IC Element's Human Resources (HR) systems, and manage PE and NPE Public Key Infrastructure (PKI) certificates via each element's Certificate Authority (CA), each of which is a sub-CA to the single IC root CA. The IC enterprise attribute services can be integrated with protected resources (PRs) via well-defined APIs, and in some cases via SAML, OIDC, or SDKs. The IC enterprise authentication and authorization services, where provided, can protect resources via an API gateway or via SAML, OIDC, and/or an SDK.

These IC enterprise ICAM services are mature and feature-complete, having been deployed for multiple years and through multiple versions.

The Four Issues

Consumers Not Being Able to Get the Data They are Legitimately Authorized to Consume

The issue of consumers not being able to get the data they are legitimately authorized to consume is due to the de-coupling of cloud vendor-provided ICAM capabilities from the IC- and DoD-provided enterprise ICAM services. This de-coupling results in consumers having to be pre-provisioned in each cloud vendor's Identity and Credential Management service – per system authorization boundary – to be able to access government-owned resources on their clouds. The pre-provisioning includes the consumer's identity, credentials, and authorization attributes. At best, this de-coupling and pre-provisioning is a duplication of effort, and at worst will enable differing attributes and attribute values for consumers and nonstandard data tagging across the different clouds, and even across different deployed systems, all leading to non-reusable, cloud vendor-specific access control policies.

Note that the reason consumers will have to be pre-provisioned per system, even though the system may be leveraging the cloud vendor's ICAM services, is that those ICAM services are designed to be isolated by tenant. For example, assume two systems deployed on Azure, system A from program A and system B from program B, and both systems leverage the Azure ICAM services. Also assume user "Fred" requires access to both system A and system B. In this case, Fred would need to be provisioned in Azure's ICAM services twice, once for system A, and again for system B. This is because program A is a different tenant than program B, and the Azure ICAM system internals are organized by tenant. This makes sense when the tenants are different companies, but not when the tenants are different programs within the same company.

This problem could be mitigated if the cloud vendor-provided ICAM services are federated with the enterprise ICAM services. In this case, the same identity and associated attributes and credentials are used across tenants within a given cloud and across clouds.

Reduced Security

The issue of reduced security is due to the increased complexity that results from each of the C2E vendors differing ICAM implementations (complexity and security are inversely related to each other). These differences encompass the APIs, user interfaces, SDKs, and paradigms for integration. For a given program that is deploying across multiple cloud vendors, the program have to have expertise in each of the cloud provider's ICAM services. For a given IC element, the assessors, Information System Security Officers (ISSOs), Information System Security Managers (ISSMs), and Information System Security Engineers (ISSEs) will need to understand each cloud provider's ICAM systems to be able to properly assess a program that is deploying on one of those clouds.

WHEN IT COMES TO SECURITY, COMPLEXITY IS NOT YOUR FRIEND

When it comes to security, complexity is not your friend. Indeed it has been said that complexity is the enemy of security. This is a point that has been made often about cybersecurity in a variety of contexts including, technology, coding, and policy. The basic idea is simple: as software systems grow more complex, they will contain more flaws and these flaws will be exploited by cyber adversaries.[2]

Increased Costs

The issue of increased costs is due to the loss of cloud portability for Information Technology (IT) systems that implement their ICAM needs using a specific cloud vendor-provided ICAM service. In other words, an IT system that is deployed on one vendor's cloud will not be able to be redeployed on a different vendor's cloud without changing the IT system to be able to integrate with the new cloud vendor's ICAM services. The benefit of multiple cloud vendors competing for hosting IC element applications is thus reduced by cloud vendor lock-in.

Note that this lock-in is not unique to the ICAM services but exists (and increases) for any cloud vendor-specific service invoked or used by an IT system.

Misalignment with Stated Enterprise Architecture Goals

According to the *Improving Cybersecurity for the Intelligence Community Information Environment Implementation Plan*, dated August 2019, from the Office of the Director of National Intelligence (ODNI), and the *DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0*, dated June 2020, from the DoD Chief Information Officer (CIO), both the IC and the DoD are moving toward aligning with the Federal Identity, Credential, and Access Management (FICAM) Architecture which explicitly identifies certain ICAM capabilities to be managed at the enterprise level vs. at the local level.[3] In addition, the recently published *DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, Version 1.0*, June 2020, and the National Institute of Standards and Technology (NIST) Special Publication 800-205 *Attribute Considerations for Access Control Systems (nist.gov)*[4] also identify specific ICAM capabilities to be managed at the enterprise level vs. at the local level. Leveraging the cloud vendor-provided ICAM services for protecting government-owned resources without federating them with the enterprise ICAM services would be moving management of those ICAM services to the local level instead of at the enterprise level. This is directly opposite what is explicitly defined in the DoD and IC enterprise architecture and policy.

Recommended Actions

The IC should consider adopting the following actions:

- Document the specific 800-53 controls that a program will inherit when they leverage the enterprise ICAM services.
  - Per ICAM service.
  - Pre-coordinate with each IC Element's assessors and approval authorities.
- Add text to the Cloud Integration and Multi-Cloud Management (CIMM) contract or Statement of Work (SOW) that would require the winning vendor to advise and train intelligence agencies (i.e., users of the C2E services) to leverage the enterprise ICAM services.
- Require each of the IC Enterprise ICAM service providers to create and publish developer guides for how programs can leverage their ICAM services.
- Provide links to the developer guides on each network fabric (U/S/TS) and on the C2E site.
- IC CIO should consider establishing a working group to evaluate each of the enterprise ICAM service provider offerings to identify any obstacles to programs leveraging their ICAM services.
  - Ensure that the working group or red team includes software developers.
- Set up education for IC Element Risk Management Framework (RMF) security assessors to enable them to better understand the enterprise ICAM services and how programs should leverage them.
- Specify by policy that government applications must use enterprise ICAM services.

The IC has made great strides in getting IC consumers access to data they are legitimately authorized to consume. Let's take specific action to ensure continued progress in data access and improved security at reduced cost as cloud vendor options expand.

Appendix A Cloud Vendor Provided ICAM Services

Amazon Web Services Commercial Cloud Services

Amazon Web Services (AWS) **Identity and Access Management (IAM)** is a way of managing what users, or non-person entities (NPEs), have access to which AWS services. Effectively, AWS IAM is for privileged users. From the AWS IAM website (AWS Identity & Access Management - Amazon Web Services): “AWS Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.” AWS IAM also provides what they call ABAC, where the attributes are based on tags that an administrator assigns to AWS resources via the AWS admin console. Finally, AWS IAM can be integrated with Active Directory.

AWS Cognito is a way of managing which users (but not NPEs) can access applications hosted on AWS. From the AWS site What Is Amazon Cognito? - Amazon Cognito:[6]

> *Amazon Cognito provides authentication, authorization, and user management for your web and mobile apps. Your users can sign in directly with a username and password, or through a third party such as Facebook, Amazon, Google, or Apple.*
>
> *The two main components of Amazon Cognito are user pools and identity pools. User pools are user directories that provide sign-up and sign-in options for your app users. Identity pools enable you to grant your users access to other AWS services. You can use identity pools and user pools separately or together.*

Azure

Azure Managed Identities is a way of managing which users or NPEs have access to which Azure services. From the Azure Managed Identities website:[7]

> “A common challenge for developers is the management of secrets and credentials used to secure communication between different components making up a solution. Managed identities eliminate the need for developers to manage credentials. Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens. For example, an application may use a managed identity to access resources like Azure Key Vault where developers can store credentials in a secure manner or to access storage accounts.”

Azure Managed Identities advertises Role Based Access Control (RBAC) only.

Azure Application Management SSO is a way of managing which users and NPEs can connect to Azure-hosted applications. Azure Application Management SSO provides an Identity Provider (IP) that applications can connect to via OIDC, SAML, User ID/Password (UID/PWD), Linked, etc.

Appendix A (cont'd.)

IBM

IBM Access Management is a way of managing which users or NPEs have access to which IBM cloud resources. From the IBM Cloud Access Management website:[9]

> "Access management enables you to control which users see, create, use, and manage resources in your account. To grant access, you can assign roles that allow users levels of access for completing platform management tasks and accessing account resources."
>
> "The way that you manage access in IBM Cloud® depends on the type of resource that you want to assign access to. IBM Cloud Identity and Access Management (IAM) is the access management system that is used for consistently managing resources that are organized in a resource group across the IBM Cloud platform. Classic infrastructure and Cloud Foundry resources are not managed by using Cloud IAM. These resource types have their own access management systems."

IBM App ID is a way to provide authentication to your cloud hosted apps.
App ID is an OIDC identity provider (IdP). From:[10]

> "When you are developing a web application, you can use the IBM Cloud™ App ID web flow to securely authenticate users. Users are then able to access your server-side protected content in your web apps."
>
> "Web apps often require users to authenticate to access protected content. App ID uses the OIDC authorization code flow to securely authenticate users. With this flow, when the user is authenticated, the app receives an authorization code. The code is then exchanged for an access, identity, and refresh token. In code, exchange step the tokens are always sent via a secure backchannel between the app and the OIDC server. This provides an extra layer of security as the attacker is not able to intercept the tokens. These tokens can be sent directly to the web server hosting application for user authentication."

Google Cloud

Google Cloud provides two separate ways of managing identities and permissions.

Identity and Access Management (IAM) is a way of managing access to Google Cloud resources. From the Google Cloud IAM website: "IAM can be sync'd with Active Directory."

Google Cloud Identity is a way of managing end users and their devices, and their accesses to applications hosted in the Google Cloud. Basically, it acts as a SAML and OIDC Identity Provider (IP) that is both pre-integrated with many cloud-based applications and allows for integrating with new applications that you may want to host on the Google Cloud. When integrating a custom application with Google as the IdP, the integration only supports SAML (i.e., no OIDC). Google Cloud Identity does support federation with other IdPs.

Oracle Cloud

Oracle Cloud Infrastructure **Identity and Access Management (IAM)** is a way of managing which users or NPEs have access to which Oracle cloud resources. From the Oracle cloud IAM website: "Oracle Cloud Infrastructure Identity and Access Management (IAM) lets you control who has access to your cloud resources. You can control what type of access a group of users have and to which specific resources." Oracle Cloud IAM can integrate with Azure Active Directory (AD).

Oracle Identity Cloud Service is an OIDC IdP that can be used to authenticate end users for Oracle cloud hosted applications. From: "Oracle Identity Cloud Service manages user access and entitlements across a wide range of cloud and on-premises applications and services using a cloud-native, identity as a service (IDaaS) platform." Oracle Identity Cloud Service can integrate with AD and other IdPs.

Notes

1. The definitions of these ICAM services are provided by the Department of Defense (DoD) Enterprise Identity, Credential, and Access Management (ICAM) Reference Design, and the Director of National Intelligence (DNI) Information Sharing Environment (ISE) Introduction to ICAM Principles.https://www.dni.gov/files/ISE/documents/DocumentLibrary/INTRO-TO-ICAM.pdf.

2. Chang FR. Is Your Data on the Healthcare.gov Website Secure? Written Testimony, U.S. House of Representatives, November 2013. http://docs.house.gov/meetings/SY/SY00/20131119/101533/HHRG-113-SY00-Wstate-ChangF-20131119.pdf (7 May 2021, date last accessed).

3. FICAM Playbook, Identity Management (idmanagement.gov). https://playbooks.idmanagement.gov/arch/identity/

4. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-205.pdf.

5. https://aws.amazon.com/iam/.

6. https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html.

7. https://docs.microsoft.com/en-ca/azure/active-directory/managed-identities-azure-resources/overview.

8. https://docs.microsoft.com/en-ca/azure/key-vault/general/overview.

9. https://cloud.ibm.com/docs/account?topic=account-cloudaccess.

10. https://cloud.ibm.com/docs/appid?topic=appid-web-apps#web-apps.

11. https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm.

12. https://www.oracle.com/security/cloud-security/identity-cloud/.

Authors

Chris Bashioum: In his 30 years of experience in the software industry, Chris has always stayed close to the code. He seeks to understand the theoretical, and then apply it to the practical hands-on of implementation. He is also keenly aware of the importance of cyber security and is a huge fan of both MITRE ATT&CK and D3FEND.

Cheryl Clopper: As the Analysis Division Chief Engineer at the MITRE Corporation, Cheryl leads and guides high impact technical work. She accelerates cloud computing implementation for mission needs with software prototypes and applied systems engineering across the IC and the military's Combatant Commands.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community's analytical workforce as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the IC's analytical community in the post-COVID-19 world.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

MITRE

SEPTEMBER 2022