IAM for the Cloud Era

Identity & Access Management in the cloud: findings and recommendations for action from the discussion hosted by iC Consult and Ping Identity

Focus of the discussion:

- IAM in and for the cloud
- IAM environments with multiple identity types
- Today's cloud consumption models
- IAM for critical infrastructures
- Challenges of IAM in M&A scenarios
- Trends in identity verification

Around the world, companies are driving the digitalization of their infrastructures Critical business processes are increasingly shifted to the cloud to make work more agile, productive, and efficient. As a result, secure, seamless end-to-end management is rapidly gaining importance.

If you want to reliably rule out the possibility of unsecured remote access being used for attacks and data theft, you are even more dependent on robust and user-friendly IAM solutions for managing customer, partner, and employee identities inside and outside of the cloud.

To address this urgent topic, iC Consult Group GmbH, together with the manufacture Ping Identity, organized a virtual roundtable on "IAM for the cloud era". Mehmet Yaliman, solutions architect at Ping Identity, and Heiko Huetter, CEO of Service Layers, led the discussion and gave practical tips and advice to the invited enterprise customers. All participants were invited to share their views and experiences of Identity & Access Management.

In the hour-long discussion, the participants addressed several exciting questions that went beyond the roundtable and highlighted key trends and solution strategies for IAM.

IAM in and for the cloud

1. Migration to the cloud usually entails a significant increase in the vulnerability. What is IAM's role in protecting critical data in cloud applications?

In today's increasingly complex hybrid environments, data access is becoming less and less visible – which increases the risk of critical data breaches. Therefore, many companies are opting for a Zero-Trust approach, in which all data accesses are considered insecure until the identity of the user (or, in the case of API access, the

IAM environments with multiple identity types

external system) has been verified. When asked, the participants shared that they still take a wait-and-see approach to this model. Nevertheless, the roundtable quickly came to consensus: Robust IAM that clearly regulates who is who, and who is allowed to do what, is indispensable for a secure connection to the cloud.

As the participants also pointed out, "IAM and cloud" is not just about managing identities when accessing cloud applications ("IAM for the cloud"). An equally important aspect is that more and more IAM systems are themselves cloud-based ("IAM in the cloud"). This is a challenge for many IT departments and must be kept front of mind.

2. Today, companies need to manage individual access rights for multiple identity types (customers, employees, partners, suppliers, etc.). Should these roles be managed in dedicated systems, or is it more efficient to consolidate them into one solution?

Several participants confirmed that they are currently dealing with this issue, and would like to bring the identity types together in a unified solution. However, most stated that they still divide the communities according to roles (typically: end customer, employee, and partner) and use a dedicated solution for each group. This strict separation is not considered ideal, as roles are increasingly blurring and many customers have access to APIs that were once exclusively for employees. One participant also noted that partners should not be grouped together generally, but rather subdivided according to the type of collaboration, the skillset, and the services used.

The complexity of this topic became even more clear when one participant pointed out that, in his company, identities are not only differentiated by type, but that several divisions also have dedicated IAM systems, which has led to a mix of very different systems and identities. However, the unification of these systems has high priority.

3. When integrating a modern IAM solution, companies can currently choose from several deployment options. What are they?

The first step for companies when integrating an IAM solution is to decide whether they favor a solution that is fully cloud-based, hybrid, or on-premises.

Those opting for a cloud-based Identity-as-a-Service model can, in the simplest case, implement a largely standardized multi-tenant solution such as Ping One, where all components and services are pre-selected and pre-configured. For customers who want a greater degree of control and choice, more customizable single-tenant solutions are available: Ping One Advanced Services, for example, offers comprehensive customization options such as the IAM platform from Service Layers.

Today's cloud consumption models

Those who do not want to switch their complete Identity & Access Management to the cloud can choose from numerous hybrid models, in which some components of the solution are hosted in the company's own data center, and others are accessed via SaaS. Which areas are outsourced, and which are operated in-house, is entirely up to the company itself. Ultimately, the composition of the hybrid model depends on the customer's individual requirements. According to the participants, a "one size fits all" model is not an appropriate solution.

Last but not least, there are classic on-prem solutions, where control and responsibility usually lie largely with the customer. Why these still are the best option for many environments becomes apparent in the further course of the discussion.

4. Not every type of company can use a cloud solution. Why?

A participant from the military industry stated that cloud-based IAM is currently not an option, due to compliance reasons.

Considering the company's highly critical data, digital identities must be managed exclusively on-premises. The use of a cloud would be unsuitable in this area. To benefit from the possibilities of cloud technology in some areas, however, the company has implemented its own private cloud, hosted in the company's own data center. However, the company has successfully used Ping Directory as an alternative to common LDAP directories. In light of the progress made in cloud security, it's possible that the strict compliance requirements may eventually change.

Another participant in the round intervened and confirmed that this is certainly possible. He has been working with companies in the military industry for some time and has already implemented cloud projects with them.

5. What IAM aspects should be considered following a merger or acquisition?

Some participants shared their experience with consolidating IAM architectures after mergers and acquisitions (M&A). A number of specific challenges need to be considered. Until now, the discussion primarily focused on security; now, the focus shifted to dealing with large volumes of data. According to the panel, an IAM solution must always focus on holistic solutions in order to meet the requirements of globally active companies – for example, when thousands of identities, groupings, and systems need to be standardized and unified following a merger.

IAM for critical infrastructures

6. What are the current options for verifying identities in the cloud, and what trends are emerging?

Generally, the Ping Stack was very well received in the discussion group. Several participants confirmed that their companies already use large parts of the Ping portfolio (Ping Directory, Ping Federate, Ping One) to manage their identities and accesses. Although the participants agreed that the Ping Stack can show its strengths especially in cloud-based environments, two participants reported that they use the solutions partially or completely on-prem. One justified this with the military industry's compliance requirements, the other stated that migration to the cloud is firmly planned, but not yet completed.

Challenges of IAM in M&A scenarios

The participants shared a wide range of Ping use cases and deployment options. The overall tenor: There are still numerous on-prem applications in IAM, but the trend is clearly moving towards cloud-native architectures. Many of the companies are already using multi-cloud services and multiple IAM providers to cope with increasing data volumes and requirements. In addition, the expectations of end customers must also be considered. Finally, it is important to find the right balance between company security and the desire for an easy-to-use IAM solution.

At this point, one participant referred to a trend that has developed in China and is now increasingly shaping the discussion in the USA: the possibility of logging into multiple communities with a single identity. The topic of single sign-on is coming into focus.

7. Do passwords have a future in Identity & Access Management?

Trends in identity verification

At the end of the discussion, one participant asked whether passwords are still up-to-date and secure for confirming identities. The group agreed: No, they are not. Passwords are neither secure(credential theft repeatedly leads to loss of valuable data) nor user-friendly (password resets continue to incur enormous costs). As a possible alternative, one participant brought up SMS confirmation, which, for example, is popular in China. But the panel disagrees: This is also no longer a modern method. Instead, the participants favored multi-factor authentication, push notifications, and biometric measures such as fingerprints. Nevertheless, some participants remained skeptical: The discussion about the end of passwords has been going on for over ten years and there is still no solution in sight.

Conclusion: Challenges can be solved with the right partners

After sixty exciting minutes, the participants were largely unanimous: Companies will be concerned with the topic of Identity & Access Management for a long time to come. After all, those responsible are facing the challenging task of developing customized solutions that are not only meet the demands of their own stakeholders, but also fulfill a wide range of strict legal and industry-specific requirements. (e.g. CRITIS). Contemporary IAM solutions, such as the broad Ping Stack or the IAM platform from Service Layers, can already map all of these requirements today. In view of the overall project complexity, companies are advised to involve experienced consultants and integrators at an early stage.

Start your IAM Cloud Journey now

www.iam-cloud-journey.com

Whether public, private, or hybrid – the IAM Cloud Journey from iC Consult lets you take your IAM to the cloud with ease! Our solution packages include everything you need for your cloud migration. From high-level recommendations by our experts to your own structured roadmap including a transition plan and timeline.

About iC Consult

iC Consult is the world's leading independent consultancy, systems integrator, and managed services provider for Identity & Access Management with more than 800 employees worldwide.

We are committed to excellence and innovation, and with the best-in-class technology in the IAM space, we provide our customers with next-level cybersecurity solutions. Our service portfolio covers Managed Services for IAM including advisory, architecture, implementation, integration, support, and operations.

iC Consult is headquartered in Germany with offices in Switzerland, Austria, France, Belgium, Spain, Bulgaria, the UK, the U.S., Canada, India, and China. The world's largest brands trust in our expertise, to secure and manage their most valuable assets: their identities.

More information at www.ic-consult.com