Contemporary Directory Services: A Study of Cloud Oriented Directory-as-a-Service

Saima Mehraj* and M. Tariq Banday**
*-**Department of Electronics & Inst. Technology, University of Kashmir, Srinagar, India
Email: saima_mehraj2003@yahoo.com, sgrmtb@yahoo.com

Abstract: Identity and access management is an advanced field which offers a number of solutions to store identities and provide access to information and communication technology resources. Currently, organizations leverage a variety of make-as-you-go solutions to manage their entire Identity Management infrastructure. Since directory services are at the center of the information and communication technology market, it needs immediate attention from the research community. This paper focusses on the importance and good understanding of directory services, which form the basic building block of an efficient identity and access management. It also examines different types of traditional on-premise directory services solution to identity and access management. Furthermore, this paper discusses a new wave of cloud-based directory services solution commonly known as Directory-as-a-Service (DaaS). DaaS solutions are cloud-based directories which are delivered on a Software-as-a-Service (SaaS) business model and have an inherent advantage of least maintenance of directory due to its service oriented nature.

Keywords: Cloud Computing; Identity Management; Active Directory; LDAP; Directory-as-a-Service.

Introduction

Cloud computing is a model of service that provides a convenient means to utilize high IT infrastructure as a utility over the internet. It offers elastic resources with dynamic provisioning and scaling based on user demands at low cost. Furthermore, cloud computing is based on pay-as-you-go pricing prototype that lets different organizations to outsource their data, applications and IT services to a third-party provider [1]. Therefore, cloud computing is envisioned as a computational environment that relies on sharing of resources to achieve coherence and economy of scale [2]. Cloud computing leverages various concepts such as, Autonomous Computing, Virtualization, Web 2.0, Utility Computing, Service Oriented Architecture (SOA), Grid computing, etc. [3] and therefore, contribute to the anatomy of cloud computing.

Despite of all the enthusiasm surrounding the cloud, many organizations and research communities are reluctant in completely trusting the cloud computing to shift their digital assets such as, data, applications, and IT services to the third-party service providers [4]. However, the services provided by third-party providers entail different security threats. Therefore, security is one of the main issues which reduces the growth of cloud computing. It is pertinent to mention here that the issues of managing the sensitive identity credentials have become a matter of concern for a large number of organizations [1]. In cloud paradigm, the issues of identity management and access control becomes more challenging due to the distributed and multi-tenant nature of cloud computing.

Identity Management facilitates the right entities to access the right resources at the right times and for the right reasons. Identity management infrastructure, in cloud environment makes sure that the user's identity is protected and the appropriate access to cloud infrastructure is made by the users [5]. It is exceptionally significant to keep track of the user's identity and control unauthorized access to the data stored on cloud infrastructure. Therefore, organizations and research communities are motivated to reconsider the identity architecture which calls for strong identity foundation. Moreover, a number of components of identity management architecture has been demarcated by the Cloud Security Alliance (CSA) SECaaS in which one of the core module has been recognized as directory services [6]. A Directory Service is a shared information infrastructure that functions as a single point from which users can locate different network resources and services. Therefore, the main aim of this paper is to put forth the importance of directory as a service which is a cloud-based SaaS solution to connect all IT resources to a single master directory in cloud environment.

The rest of this article is organized as following: section I elaborates the concept of cloud computing focusing on Identity and Access Management; section II discusses the survey related work; section III specifies the directory services in general, its benefits, traditional and modern directory services available; section IV explains authentication services using directory services; and, section V emphasizes on directory-as-a-service followed by discussions and conclusion.

Related Work

This section reports recent research works carried out in identity management systems especially directory service solutions in cloud environment.

Umme et al in [1], examined various cloud based Identity Management Systems (IDMS). In this paper, authors investigated various IDMs in order to know the security issues in the respective field. The authors also explained various aspects such as, reliability and applicability of various cloud based Identity infrastructure. In addition, the author has detailed a list of attacks which occur in cloud-based IDMSs. This work has led to the progress of an efficient and secure Cloud based IDMS.

Deepak et al in [5], highlights the issue of security that is delivered as cloud services. The authors have proposed security-as-a-Service and elucidates its compatibility with prominent cloud features including elasticity, pay-per-use, and portability service. The authors conclude by mentioning that solution can work best with existing on premise platform based solutions to augment their security capabilities.

Sonam et al in [7], elaborated the dynamic management of user's identity federation. The authors holistically specify the various trends and approaches which are leveraged towards a better Identity Management infrastructure in cloud computing. The authors also postulate that in cloud environment Identity management infrastructure can have several types of implementations. The authors conclude by declaring that the organizations need to ensure that the users are properly authenticated and authorized to different resources using strong Identity infrastructure.

Khalid et al in [8], designed a protocol for authentication and authorization that points out the main features of anonymous public key certificates communication in the cloud. The author in addition, surveys some of the open industrial solutions available such as, Open ID, Shibboleth etc. Besides, authors proposed protocol can be integrated with existing identity management infrastructure and therefore, using this protocol real identity is never disclosed in two communicating parties and thus, the communication becomes transparent to the users.

Marczak et al in [9], have elaborated on the directory services theory in detail. The authors have discussed directory service and its evolution in detail. The authors also specified directory services configurations. The authors have also given a detailed description on how directory services relate to managed preferences. In conclusion, the authors have provided the conceptual framework and critical technical information on directory services in the network infrastructure.

Cheng et al in [10], have mentioned a detailed research on Directory Services System. The author makes explorations on the main research content of digital resources directory service system. The author also discusses the mechanisms, the theory, construction of the rules of the digital resources directory services. The author also proposes a new concept of knowledge resource directory service.

Pradeep et el in [11], explained authentication and data privacy aspect in cloud computing. The authors propose a Group Key Authentication (GKA) protocol for preserving data privacy. The authors have also evaluated the effectiveness and correctness of the protocol. The authors also specify that identity privacy is significant model in data sharing and where data encryption is not feasible. Authors conclude by stating that the scheme appreciates with necessary control for authentication for multi-groups.

Jian et al in [12], elaborated on access control and user authentication. The authors have proposed a novel lightweight identity authentication based access control scheme for cloud computing. In conclusion, the authors remark that this scheme transfers the main computation to the authorized agency and therefore, this scheme is more efficient than other access control schemes.

Nevertheless, the directory services delivered as a service for Identity Management infrastructure has not been evaluated by research community so far. As defined by Cloud Security Alliance Implementation Guidance-Category 1, directory services being the basic building block of Identity Management, therefore, requires substantial consideration from the research community.

Identity and Access Management using Directory Services

Directory Services

Directory service is, indeed, one of the basic building blocks of Identity Management infrastructure [13]. It is reflected as a primary element of any network. A Directory Service is an information store that maps users, IT resources, and the relationship and access between the two, in one central location. Furthermore, directory services are at the core of every IT organization, and are important because user access is mapped to the specific applications and devices. Thus, organizations that leverage a well-organized and structured directory services have better control and visibility over their infrastructure [14].

Nevertheless, directory services started times ago when X.500 protocol was designed. The X.500 protocol is an open standard that includes directory services. However, the most notable implementation is the open source standard Lightweight Directory Access Protocol (LDAP) which was introduced in 1993. LDAP helped making implementation of directory services simpler, and easier, and thus, a number of LDAP-based directories emerged. In addition to this, directory is queried in the form of Kerberos, SAML, OAuth, or a wide variety of authentication protocols.

Typically, a directory contains more descriptive and attribute-based data that is concise and strictly relevant to an entry. A directory is a collection of entries, which consist of one or more attributes each. Each attribute has one or more values and a type that determines the kind of information the values can hold. However, the entries in a directory are arranged hierarchically in a tree like structure which are represented by its entry name, or relative distinguished name (RDN), and by its distinguished name (DN) [15]. Moreover, directories may replicate data in order to increase availability and reliability, and reduce response time. However, when directory data is replicated, temporary inconsistencies between the replicas may be acceptable as long as all the replicas are updated eventually. In addition, directory information can be accessed by using APIs that allow client applications to search and retrieve information from the directory server, as well as modifying the directory entries if such modifications are allowed.

Benefits of Directory Services

Directory services ensure that only right people have the right access to the organizations IT resources. It frees the IT admins from the time-consuming hassles of managing on premise directories [14]. Therefore, the main goal of directory services is to manage users, authenticate, and authorize to different devices and applications. Management of user accounts is perhaps the most critical activity in any organization. User management is an operational function of connecting users to the IT resources, and incorporate two significant roles: authentication and authorization. Authentication is an essential part of an organization's network that makes sure that the right people have right access to the right machines. Therefore, authentication controls access to IT resources such as, devices, files, IT applications, Web applications, etc.

Likewise, authorization is another granular aspect in directory services where access is controlled to IT resources. For instance, a server can have multiple levels of access such as, root-level access, read access, read/write access, and file/directory access level. Also, an IT application can have admin level access where the administrator can create and terminate other users, or even make changes to the system or configuration. Equally, a user of that application may have read level access only. Therefore, all of these differing levels of access are part of directory services authorization. Therefore, directory services form a critical component in the modern era where identity theft and user credential compromises are very common [9, 10].

More importantly, there can be a number of information sources in an organization, therefore, providing directory services as a single authoritative source will reduce complexity and also lowers cost. Moreover, the overhead of managing identities in various applications can be eliminated by setting up different applications to a single central directory service. Additionally, authentication of users to various databases can also be accomplished using one directory service reducing the burden to manage user credentials for each database instance.

Traditional Directory Services

Identity and access management (IAM) is a broad IT term that encompasses everything from the management of identities, resources and user access [16]. At the center of the IAM is the directory service solution that provides a greater control, visibility, and security to the IT infrastructure [14, 17]. However, the different types of traditional directory services available include:

Microsoft Active Directory (AD)

Active Directory is a directory service developed by Microsoft for Windows domain networks. It authenticates, authorizes, and manages users in a Windows domain network that assigns and enforces security policies for all machines. For instance, when a user logs into a computer that is part of a Windows domain, AD checks the submitted password and determines the access level of the user. Further, AD also enables single sign-on access to internal Windows based resources that is once a user logs onto the device connected to the network helps users access resources on the network.

Lightweight Directory Access Protocol (LDAP) Directory Services

LDAP is the leading directory service protocol standard and has become a core protocol for user directories. LDAP provides a central place to store usernames and passwords. This allows different applications and services to connect to the LDAP server to validate users. Moreover, LDAP directory service is based on client-server model. One or more LDAP servers contain the data making up the LDAP directory tree. An LDAP client connects to an LDAP server and requests for some information. The server provides the information, or refers the client to another LDAP server that may be able to provide the information. Furthermore, LDAP is designed to allow speedy and efficient access to the directory and is therefore, leveraged by organizations worldwide. OpenLDAP is open-source implementation of the LDAP.

Limitations of Traditional Directory Services

At first glance, a major drawback with traditional directory services is that they are outdated and time consuming to work with. In addition, some other shortcomings of the traditional directory services are discussed below:

Microsoft Active Directory

- AD is operating system dependent that is it is compatible only with Windows machines and offers no means to manage non-Window clients or servers.
- AD has high maintenance costs and is very difficult to integrate into pre-existing network systems.
- AD if somehow goes down, entire network will go down.
- AD takes a lot of time to install and configure.
- AD is complex and has high infrastructure costs.
- AD is very difficult to integrate into the cloud.

LDAP Directory Services

- Setting up and managing an LDAP directory is more complex and requires careful planning.
- A directory server (LDAP) server cannot be its own client that is, the machine running an LDAP server software cannot be configured to become an LDAP client.
- LDAP is not optimal to store dynamic information.

Due to these shortcomings of traditional directory services, there is a serious need for innovation within the directory realm.

Modern Directory Services

In today's modern era, organizations require fast access to data and at the same time efficient relationship among employees, partners, and the end users. Moreover, the architectural difficulty of identity management infrastructure increases regulatory requirements and privacy concerns making management of identities and access levels a significant business challenge. Therefore, complex and identity related business challenges require efficient and next generation directory services which include [18, 19]:

Microsoft Azure Active Directory (AD)

Azure Active Directory (Azure AD) is Microsoft's cloud based directory which provides comprehensive identity management solution. It combines core directory services, and advanced identity and access management capabilities to manage users and different groups. Moreover, Azure directory provides an affordable, easy to use solution to help secure access to on premise and numerous cloud applications such as Salesforce, Dropbox, etc. In addition, Azure AD offers developers an effective means to integrate identity management solution into their applications thus helping organizations to secure their applications and reduce costs efficiently.

Amazon Web Services (AWS) Directory Services

AWS Directory service is a managed service offered by Amazon that provides directories to store information regarding the organization, users, groups, computers, etc. Moreover, AWS Directory service is supposed to reduce management tasks, thereby allowing organizations to fully focus on business rather than the IT infrastructure. Besides, it lessens the need for organizations to build complex and highly available directory architecture. In addition, data replication, software updates and patching is all handled by Amazon. AWS Directory service makes it easier to set up and run directories in the AWS cloud, thereby connecting AWS resources with an existing on premise directory infrastructure. However, once a directory is created, users and groups can be managed efficiently, providing single sign on access to all the applications and services, as well as simplify the creation and application of group policy.

Authentication using Directory Services

Indeed, authentication forms one of the integral component of Identity and Access Management (IAM). It is the verification of the user, computer, or service (such as an application on a network) that it claims to be. Authentication using directory services is a process in which the credentials provided by the authorized users are compared to those stored in a directory infrastructure. If the credentials match, the process is completed and the user is granted authorization for access, otherwise denied. The authentication using directory services include [20]:

Authentication using Active Directory

Active Directory (AD) authentication offers users a faster and more secure authentication mechanism. User authentication using Active Directory confirms the identity of a user trying to log on to a domain and lets the user access resources (such as data, application, or services) located anywhere on the network. Moreover, AD is unified with the Windows security subsystem through logon authentication in the directory. It ensures that only authenticated users can log on to the network and that each network resource is available only to authorized users. In addition, AD uses the Kerberos v5 protocol for authentication. Also, AD authentication provides a strong and easy to manage security system for a heterogeneous network.

Authentication using LDAP

Lightweight Directory Access Protocol (LDAP) is a network protocol designed for querying directory services and modifying data in a directory. LDAP authentication has become one of the enterprise user infrastructure cornerstones. As the organizations are collaborated with customers, employees, vendors, business partners etc., the need to authenticate users has significantly increased from security perspective. Moreover, LDAP authentication relies upon the LDAP directory which has the most up to date identity information with which an authentication is to be done. Furthermore, the LDAP standard specifies a protocol for communicating between LDAP clients and servers in which an LDAP client connects to an LDAP server, issues a query, receives a response, and disconnects from the server.

Directory-as-a-Service for Identity and Access Management

As already discussed, a directory confirms a user's identity (authenticates), controls user access (authorizes), and manages all the devices in an organization. A directory gives end users and employees access to the variety of IT resources they need, including applications, devices and various services. Conventionally, Microsoft Active Directory (AD) and OpenLDAP have been the principal directory service providers. Unfortunately, the aforementioned directory services are difficult to implement, and maintain by IT admins. Furthermore, AD and LDAP haven't been able to adjust to the ever-changing IT landscape of modern era. Therefore, there is a growing need to create a central user directory to free IT admins from heavy maintenance of directory services. In addition, organizations are leveraging various cloud services which urges them to move beyond the capabilities of their legacy IAM solutions.

Identities are becoming the most vital digital assets in the modern era. Therefore, the need for organizations to protect and manage digital identities has led to the new concept of Identity-as-a-Service (IDaaS) which is SaaS-based offering to use single sign-on [21], authentication and access control to provide secure access to the variety of SaaS applications. IDaaS can be integrated with the existing directory or the services can be taken from cloud based user directory [22].

A newly introduced user directory service solution has recently appeared which is generally known as Directory-as-a-Service (DaaS). Nevertheless, DaaS is a cloud-based user directory solution which is delivered on a software-as-a-Service (SaaS) business model. DaaS is the solution that solves the increasingly complicated landscape of authentication, authorization, and user management centrally. Furthermore, DaaS incorporates important factors such as multi-factor authentication, independent and varying access to services, and even manage surplus devices. In short, DaaS is a modern user directory that allows organizations to take advantage of cloud-based business infrastructures to a single master directory, while maintaining communication through a number of protocols including LDAP, Kerberos, SAML, OAuth, RADIUS, and many others [23]. For example, IT applications often use LDAP, whereas Web-applications leverage SAML or OAuth. Meanwhile windows applications utilize Kerberos. A DaaS user directory solution uses all of these protocols to connect users to their IT infrastructure and allows organizations to move on premise directory into cloud as a service to have one master directory and ensure that all of their IT resources are well maintained and controlled.

Need of Directory-as-a-Service

Today's modern organizations which are leveraging the cloud are absolutely ideal users for DaaS. These organizations need a modern solution to the directory to centrally manage and control user access. As a matter of fact, it is evident that patching the directory solutions to accommodate the changing IT landscape is very cumbersome. Specifically, while moving to the cloud solves many issues, but also creates others. For instance, cloud servers hosted at Amazon Web Services (AWS) or Google Compute Engine are currently facing problems for most on premise hosted directory solutions. Further, nowadays Macs are the fastest growing devices and therefore, not manageable for most of the organizations thereby, causing tremendous problems in management. These devices will be well managed by DaaS solution [24]. Besides, many organizations have moved to the Google cloud for emailing service but are still stuck with an on premise directory. Google's user store is not intended to be a directory with full authentication, authorization, and management services. All these challenges are motivating the innovation of DaaS.

Working of Directory-as-a-Service

DaaS is basically a cloud based Service for authentication, authorization and management of users, applications, and devices. The functions of DaaS can be summarized below [24]:

- DaaS can act as a directory of record or an extension of an existing directory. Users are authenticated using LDAP, RADIUS, SAML, or SSH protocol or using REST-based APIs. DaaS can be used on Windows, Mac, and Linux devices.
- DaaS ensures that the right users have right access to the right IT resources. It issues a command when users are added or removed.

- DaaS has the capability of managing Windows, Mac, and Linux devices at scale. DaaS solution makes the task execution on devices easier by globally updating policy and registry settings and changing system configurations.

Discussions and Conclusion

Identity and Access management (IAM) is, indeed a broad field encompassing the ability to securely store identities and provide access to IT infrastructure. These solutions have been around decades where an individual was granted access to a singular computer. At that time, IAM was simple because the identities, privileges and access was limited. As a result of which most IAM was granted and reviewed manually. However, over time managing identities and access became a complicated task as the number of people needing access and the type of IT resources increased. Therefore, IAM has become a complex field and becoming even more complex with the integration of the cloud infrastructure. Furthermore, as identities are conduit to an organization's digital assets and information, the organizations care deeply about how to secure and federate identities properly. In this regard, directory services are discussed in detail which are at the core of an organization.

Nonetheless, directory service is a critical component of the network infrastructure and therefore, is a point of authentication and authorization for a variety of IT resources and also includes device management capabilities. In fact, directory serves as the identity provider and therefore provides greater visibility, control, and security over the infrastructure of an organization. Conventional methods of directory services such as, AD and LDAP solved on premise infrastructure needs but the cost and management overhead of maintaining these legacy solutions increased with the increase in IT complexity. Additionally, the legacy directory services have to struggle to keep up with new innovations in IT market including the shift to cloud infrastructure, Web-based applications, and alternate platforms to Windows. Since these traditional directories are not able to cover all of the different platforms and geographies, new central cloud-based directory service, most often called as Directory-as-a-Service, can bridge the gap. In principal, this approach is a cloud-based directory service leveraged to ensure that access is controlled to IT resources and all the user's credentials are stored centrally.

Furthermore, DaaS is a cloud-based user directory service solution that allows organizations to place all of its users in one core, authoritative user store for more effective and secure user management. Hence, this approach results in less number of mistakes and security breaches within the user store. Moreover, users can be provisioned and de-provisioned with a single click and by consequence can have access to all of the IT resources they need for their jobs or be terminated from having access. Besides, an organization can make sure that all of its IT resources are controlled. However, cloud-based directory solution off-loads the on-going operations to third party service providers that is, the business outsources the set-up, configuration, and maintenance of the user directory. In contrast to the conventional directory services, the DaaS user directory solutions will increase security, gain control and visibility over the IT infrastructure. Another important feature of DaaS solutions are that they are cost-effective and thus, solution becomes scalable due to SaaS-based approach. Since, DaaS solutions consolidate identities into one core directory, IT resources can be easily managed and secured.

Acknowledgment

This work was supported by grants received from Ministry of Electronics and Information Technology, Govt. of India.

References

[1] Umme Habiba, Rahat Masood, Muhammad Awais Shibli, and Muaz A Niazi. "Cloud identity management security issues & solutions: a taxonomy", SpringerOpen Journal, 2014.

[2] Mazhar Ali, Samee U. Khan, Athanasios V. Vasilakos, "Security in cloud computing: Opportunities and challenges", Elsevier, Information Sciences, vol. 305, 2015, pp. 357–383.

[3] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing", SpringerOpen Journal, 2013.

[4] R. Velumadhava Raoa, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing", Elsevier, 2015 pp. 204 – 209.

[5] Deepak H. Sharma, Dr. C. A. Dhote, Manish M. Potey, Identity and Access Management as Security-as-a-Service from Clouds, Elsevier, 2015, pp. 170 – 174.

[6] SecaaS Implementation Guidance, Cloud Security Alliance, Category 1, "Identity and Access Management", 2012.

[7] Sonam Sudha, Ms.Vasudha Arora, "Identity and Access Management in Cloud Computing", International Journal For Research In Applied Science And Engineering Technology (IJRASET), July 2014.

[8] Umer Khalid, Abdul Ghafoor, Misbah Irum, Muhammad Awais Shibli, "Cloud based Secure and Privacy Enhanced Authentication & Authorization Protocol", Elsevier, 17th International Conference in Knowledge Based and Intelligent Information and Engineering Systems-KES, vol. 22, 2013, pp 680 – 688.

[9] Edward Marczak, Greg Neagle, "Understanding Directory Services", SpringerLink Apress, Enterprise Mac Managed Preferences, 2010 pp 17-27.

[10] Cheng Jiejing, Liu Xiaoxiao, Xiong Dongping, Zhang Fang, "Research on Digital Resources Directory Services System", IEEE International Conference on Information Management, Innovation Management and Industrial Engineering, 2009.

[11] Pradeep Kumar Arya, Selvamani K, Kanimozhi S, "An Authentication Approach for Data Sharing in Cloud Environment for Dynamic Group", IEEE- Internationai Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014.
[12] Jian Shen, Dengzhi Liu, Qi Liu, Baowei Wang, Zhangjie Fu, "An Authorized Identity Authentication-based Data Access Control Scheme in Cloud", IEEE- ICACT, 2016.
[13] Michael D Waters, "Evaluating Identity and Access Management (IAM) as a Cloud Service", Research Gate, September 2016.
[14] Fusion Middleware, "Identity and Access Management Suite", Oracle Directory services, Oracle Whitepaper, June 2015.
[15] https://msdn.microsoft.com/en-us/library/aa366100(v=vs.85).aspx, accessed on 24-11-2017.
[16] Issa Khalil, Abdallah Khreishah, Muhammad Azeem, "Consolidated Identity Management System for secure mobile cloud computing", Elsevier, vol. 65, 2014 pp. 99-110.
[17] Yaser Fuad Al-Dubai, Dr. Khamitkar S. D, "Kerberos: Secure Single Sign-on Authentication Protocol Framework for Cloud Access Control", Global Journal of Computer Science and Technology: B Cloud and Distributed, Vol. 14, 2014.
[18] https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview, accessed on 26-11-2017.
[19] http://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html, accessed on 26-11-2017.
[20] https://technet.microsoft.com/en-us/library/bb463152.aspx, accessed on 27-11-2017.
[21] Aniesh Krishna K, Balagopalan A S, "Authentication Model For Cloud Computing Using Single Sign-On", Proceedings of 10th IRF International Conference, 2014.
[22] Bernd Zwattendorfer, Klaus Stranacher, and Arne Tauber, "Towards a Federated Identity as a Service Model", Springer International Conference on Electronic Government and the Information Systems Perspective, 2013, pp 43-57.
[23] Nitin Nagar, Pradeep k. Jatav, "A Secure Authenticate Framework for Cloud Computing Environment", International Journal of Advanced Computer Research, vol. 4, 2014.
[24] Onelogin, "Choosing the Right Active Directory Integration Framework for your Cloud Application Portfolio", White paper, April 2014.