(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103023921 A
(43)申请公布日 2013.04.03

(21)申请号 201210580828.X

(22)申请日 2012.12.27

(71)申请人 中国建设银行股份有限公司
地址 100032 北京市西城区金融大街 25 号

(72)发明人 欧万翔 孙浩 叶坤林 朱志林廷懋

(74)专利代理机构 广州三环专利代理有限公司 44202
代理人 温旭 郝传鑫

(51)Int.Cl.
H04L 29/06(2006.01)

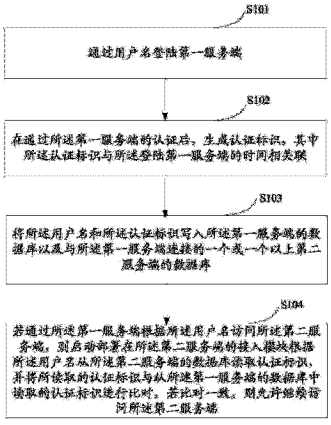
权利要求书 2 页 说明书 7 页 附图 2 页

(54)发明名称

一种认证接入方法和认证系统

(57)摘要

本发明公开了一种认证接入方法，包括通过用户名登陆第一服务端，在通过认证后，生成认证标识，其中认证标识与登陆第一服务端的时间相关联，将用户名和认证标识写入第一服务端的数据库以及与第一服务端连接的一个或多个第二服务端的数据库，若通过第一服务端根据用户名访问第二服务端，则启动配置在第二服务端的接入模块根据用户名从第二服务端的数据库读取认证标识，并将所读取的认证标识与从第一服务端的数据库中读取的认证标识进行比对，若比对一致，则允许继续访问第二服务端。本发明还提供了相应的认证系统。本发明的方法和系统实现了两种服务端之间的单点登陆，整体上提高了认证系统的集成认证效率。



CN 103023921 A

1. 一种认证接入方法，其特征在于，包括：

通过用户名登陆第一服务端，

在通过所述第一服务端的认证后，生成认证标识，其中所述认证标识与所述登陆第一服务端的时间相关联；

将所述用户名和所述认证标识写入所述第一服务端的数据库以及与所述第一服务端连接的一个或一个以上第二服务端的数据库；

若通过所述第一服务端根据所述用户名访问所述第二服务端，则启动部署在所述第二服务端的接入模块根据所述用户名从所述第二服务端的数据库读取认证标识，并将所读取的认证标识与从所述第一服务端的数据库中读取的认证标识进行比对，若比对一致，则允许继续访问所述第二服务端。

2. 如权利要求 1 所述的方法，其特征在于，还包括：

在通过所述第一服务端的认证之后，生成认证标识之前，获取所述用户名所属机构和所属角色，并将所述用户名、所述用户名所属机构和所属角色组成的认证信息写入所述第一服务端的数据库。

3. 如权利要求 2 所述的方法，其特征在于，所述第二服务端包括 Cognos 服务端。

4. 如权利要求 3 所述的方法，其特征在于，还包括：

在允许继续访问所述第二服务端之后，启动所述接入模块对所述第一服务端发送的所述认证信息进行验证，并将验证后获取的信息组装为 visa 对象，保存至所述第二服务端的数据库。

5. 如权利要求 4 所述的方法，其特征在于，所述对所述第一服务端发送的所述认证信息进行验证包括：

验证用户名是否正确，

若正确，则查询该用户名对应的认证信息，并获取该用户名所属应用的所有机构和角色。

6. 如权利要求 1 至 5 任一项所述的方法，其特征在于，所述接入模块通过 webservice 应用接口与所述第一服务端进行通信。

7. 如权利要求 1 至 5 任一项所述的方法，其特征在于，所述认证标识包括与所述登陆第一服务端的时间相关联的字符串。

8. 如权利要求 2 所述的方法，其特征在于，所述认证信息中用户名和该用户名所属机构和角色以单张数据库表的形式进行存储。

9. 一种认证系统，其特征在于，包括第一服务端、与所述第一服务端连接的一个或一个以上第二服务端、部署在所述第一服务端的生成模块和部署在所述第二服务端的接入模块，其中，

第一服务端，用于通过用户名登陆；

所述生成模块，用于在通过所述第一服务端的认证后，生成认证标识，其中所述认证标识与所述登陆第一服务端的时间相关联，并将所述用户名和所述认证标识写入所述第一服务端的数据库以及与所述第一服务端连接的一个或一个以上第二服务端的数据库；

所述接入模块，用于若通过所述第一服务端根据所述用户名访问所述第二服务端，根据所述用户名从所述第二服务端的数据库读取认证标识，并将所读取的认证标识与从所述

第一服务端的数据库中读取的认证标识进行比对，若比对一致，则允许继续访问所述第二服务端。

10. 如权利要求 9 所述的系统，其特征在于，所述第一服务端还部署有获取模块，用于在通过所述第一服务端的认证之后，生成认证标识之前，获取所述用户名所属机构和所属角色，并将所述用户名、所述用户名所属机构和所属角色组成的认证信息写入所述第一服务端的数据库。

11. 如权利要求 10 所述的系统，其特征在于，所述第二服务端包括 Cognos 服务端。

12. 如权利要求 11 所述的系统，其特征在于，所述接入模块，还用于在允许继续访问所述第二服务端之后，对所述第一服务端发送的所述认证信息进行验证，并将验证后获取的信息组装为 visa 对象，保存至所述第二服务端的数据库。

13. 如权利要求 12 所述的系统，其特征在于，所述接入模块，用于对所述第一服务端发送的所述认证信息进行验证，具体地，验证用户名是否正确，若正确，查询该用户名对应的认证信息，并获取该用户名所属应用的所有机构和角色。

14. 如权利要求 9 至 13 任一项所述的系统，其特征在于，所述接入模块通过 webservice 应用接口与所述第一服务端进行通信。

15. 如权利要求 9 至 13 任一项所述的系统，其特征在于，所述认证标识包括与所述登陆第一服务端的时间相关联的字符串。

16. 如权利要求 10 所述的系统，其特征在于，所述认证信息中用户名和该用户名所属机构和角色以单张数据库表的形式进行存储。

一种认证接入方法和认证系统

技术领域

[0001] 本发明涉及数据安全领域，具体而言，涉及一种认证接入方法和认证系统。

背景技术

[0002] 随着信息安全技术的不断发展，人们对身份安全认证意识的不断提高，对于不同级别或层次业务或操作，采用不同安全认证方案成为一种趋势。例如，在金融行业中，对于不同风险等级的应用而言，需要不同等级的用户身份认证方案，也就是说，对于同一用户而言，需要在不同应用服务之间反复的进行身份认证接入处理操作，认证效率极低。

[0003] 例如，某一银行 A 为提高报表展现效率，建立了集中显示报表服务的应用服务端，作为前端的该应用服务端以后端的多个报表服务端为支撑，集中显示后端多个报表服务端的的处理结果。然而，为确保报表数据的安全需要，一般的银行都会对不同的应用服务采用不同等级的身份认证方案，这就是说，后端的每一个应用服务采用不同认证方案的服务端接入前端的应用服务端，每次都需要为其在应用服务端和报表服务端进行一次手工配置，以将后端的多个报表服务端在集成的应用服务端上进行显示，这种认证接入配置繁琐，效率较低，导致认证服务系统的整体认证集成度低下。

发明内容

[0004] 本发明提供了一种认证接入方法和认证系统，对于采用集成的第一服务端对多个第二服务端进行展现的场景而言，在不同的应用服务即不同认证方案中，仅需在第一服务端配置一次，即可实现对第二服务端的访问，实现了在第一服务端和第二服务端之间的单点登录，提高了认证服务系统的整体集成度。

[0005] 根据本发明实施方式的第一方面，提供了一种认证接入方法，包括 ：

[0006] 通过用户名登陆第一服务端，

[0007] 在通过所述第一服务端的认证后，生成认证标识，其中所述认证标识与所述登陆第一服务端的时间相关联 ；

[0008] 将所述用户名和所述认证标识写入所述第一服务端的数据库以及与所述第一服务端连接的一个或一个以上第二服务端的数据库 ；

[0009] 若通过所述第一服务端根据所述用户名访问所述第二服务端，则启动部署在所述第二服务端的接入模块根据所述用户名从所述第二服务端的数据库读取认证标识，并将所读取的认证标识与从所述第一服务端的数据库中读取的认证标识进行比对，若比对一致，则允许继续访问所述第二服务端。

[0010] 根据本发明实施方式的第二方面，提供了一种认证系统，包括第一服务端、与所述第一服务端连接的一个或一个以上第二服务端、部署在所述第一服务端的生成模块和部署在所述第二服务端的接入模块，其中，

[0011] 第一服务端，用于通过用户名登陆 ；

[0012] 所述生成模块，用于在通过所述第一服务端的认证后，生成认证标识，其中所述认

证标识与所述登陆第一服务端的时间相关联，并将所述用户名和所述认证标识写入所述第一服务端的数据库以及与所述第一服务端连接的一个或一个以上第二服务端的数据库；

[0013] 所述接入模块，用于若通过所述第一服务端根据所述用户名访问所述第二服务端，根据所述用户名从所述第二服务端的数据库读取认证标识，并将所读取的认证标识与从所述第一服务端的数据库中读取的认证标识进行比对，若比对一致，则允许继续访问所述第二服务端。

[0014] 本发明实施方式提供的认证接入方法和认证系统，通过在登陆第一服务端后生成与登陆时间相关联的一次性认证标识，并将该认证标识和用户名写入第一服务端和第二服务端的数据库，当通过第一服务端访问第二服务端时，通过配置在第二服务端的接入模块读取两个服务端的认证标识并进行比对，比对一致后可继续访问第二服务端，通过用户名结合认证标识的方式实现了对第一服务端和第二服务端之间的单点登录，提高了认证服务系统的整体集成度。

附图说明

[0015] 图 1 图示了根据本发明实施方式的认证接入方法的示意图。

[0016] 图 2 图示了根据本发明实施方式的认证系统的示意图。

具体实施方式

[0017] 为使本发明的实施例的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述。

[0018] 参考图 1，图示了根据本发明实施方式的认证接入方法的示意图，具体而言，该认证接入方法包括：

[0019] S101，通过用户名登陆第一服务端，

[0020] S102，在通过所述第一服务端的认证后，生成认证标识，其中所述认证标识与所述登陆第一服务端的时间相关联；

[0021] S103，将所述用户名和所述认证标识写入所述第一服务端的数据库以及与所述第一服务端连接的一个或一个以上第二服务端的数据库；

[0022] S104，若通过所述第一服务端根据所述用户名访问所述第二服务端，则启动部署在所述第二服务端的接入模块根据所述用户名从所述第二服务端的数据库读取认证标识，并将所读取的认证标识与从所述第一服务端的数据库中读取的认证标识进行比对，若比对一致，则允许继续访问所述第二服务端。

[0023] 本发明实施方式中，用户通过用户名登陆第一服务端，其中第一服务端可以是为多种不同应用系统提供统一报表展现的集成的应用服务端(例如，可以是中国建设银行开发的 RIDE 服务端)，而第二服务端可以是各种行业领先的 BI 报表工具(例如，Cognos 服务端)，作为前端的第一服务端(例如，RIDE 端)以作为后端的第二服务端为支撑。在一些特定实施方式中，企业资源管理系统、统计信息管理系统等应用系统的报表展现功能不用进行单独开发，它们可以利用 RIDE+Cognos 的功能获得所有基本的报表展现服务。

[0024] 第一服务端和第二服务端之间通过 webservice 方式进行通讯，换而言之，第一服务端和第二服务端中的任意一个服务端通过调用另一个服务端提供的 webservice 接口来

取得进入的入口方式。在同一应用服务中，第一服务端和第二服务端采用相同的认证方法，而对于不同的应用服务，基于认证安全的需要采用不同的认证方法。例如，对于应用 aa 来说，第一服务端和第二服务端可以采用认证方法 AA ；而对于应用 bb 来说（其中，bb 应用是与 aa 应用不同的应用），第一服务端和第二服务端可以均采用认证方法 BB（例如，认证方法 BB 可以是与认证方法 AA 不同的认证方法）。本发明提供的认证接入方法可以在不同应用服务（也就是对应不同认证方法）的场景下，无需对各个不同应用对应的不同认证方法单独进行认证配置，而是利用统一的认证标识进行认证处理，这种认证接入方法显著改善了认证处理的接入效率，特别在第二服务端个数较多（换而言之，对应应用服务数目较大）的场景中。

[0025] 在通过用户名登陆第一服务端后进行认证处理，不管采用的是何种认证方案，当然前提是已经在第一服务端配置完成相关认证信息，在该用户名通过第一服务端的认证后，第一服务端记录该用户名的登陆状态为“已成功登陆”。

[0026] 在该用户名通过认证后，第一服务端部署的生成模块将为该用户名生成认证标识，该认证标识与该用户名登陆第一服务端的时间相关联，也就是说，该认证标识随用户名登陆第一服务端的时间变化而变化，同一用户名在不同时间点登陆第一服务端所生成的认证标识不同。这种方式生成的认证标识可确保认证标识的实时性和唯一性，提高认证接入的安全性。在本发明的一些实施方式中，认证标识可以是与登陆第一服务端的时间相关联的字符串，例如，可以是 32 位的随机字符串。本领域技术人员可采用能实现上述目的的任何形式的认证标识，并不限于本文中提到的实施方式。

[0027] 然后，将用户本次登陆的用户名和该用户名本次登陆第一服务端生成的认证标识一起写入第一服务端的数据库，同时写入与第一服务端连接的一个或一个以上（例如，两个、三个或更多个）第二服务端的数据库。本发明实施方式中的第二服务端可以是 Cognos（国际商业机器 IBM 公司的 Cognos）、MSTR(Microstrategy)、BO（Business Object）等专业商务智能（Business Intelligence，BI）报表工具服务端。

[0028] 本发明实施方式中，在通过第一服务端认证之后，生成认证标识之前，还包括，从认证的数据库中获取该用户名所属机构和所属角色，以及该用户名所属应用的所有机构和所有角色，并将该用户名、该用户名所属机构、该用户名所属角色组成认证信息，然后将组成的认证信息以及该用户名所属应用所有机构和角色写入第一服务端的数据库（例如，oracle 数据库），以便后续管理用户对第一服务端进行权限管理。例如，对于银行目前使用的各种认证系统，一般要求用户具备所属机构和所属角色，以此来区分用户所应授予的权限，以 libin.xm 为例，其所属机构可认为是“厦门分行”，所属角色为“会计部门一般查询人员”，则授予 libin.xm 的权限为查看厦门分行会计部的数据，而不能进行其他操作，如不能对所查看的数据变更修改，也不能查看此机构之外的数据。例如，某张报表“存款明细表”，在应用管理员对该报表授权时，第一服务端会将所有机构及所有角色列出，方便管理员从中选择出来进行授权（比如授予某个机构中的某个角色具有查看和删除该报表的权限）。其中，同一用户名以及该用户名所属机构和角色以一张数据库表的形式保存在数据库中，而该用户名所属应用的全机构、全角色各自以一张数据库表的形式在数据库中进行存储。

[0029] 需要说明的是，当用户退出第一服务端后，除了该用户名所属应用的全机构、全角色之外的其他信息，例如本次登录生成的认证标识、该用户名所属机构和角色等都会删除，节省了存储空间，也有利于减低数据库中存在多个认证标识而导致的查询压力。

[0030] 用户在第一服务端登陆后，可以根据用户名通过第一服务端访问第二服务端，若通过第一服务端根据用户名访问第二服务端，则启动部署在第二服务端的接入模块，接入模块根据访问第二服务端的用户名从第二服务端的数据库中查询该用户名对应的认证标识，并将从第二服务端数据库读取的认证标识与从第一服务端数据库读取的认证标识进行比对，若比对一致，则该接入模块可以通过向第二服务端反馈认证通过来允许继续访问第二服务端。本发明实施方式中，正常情况下，第一服务端和第二服务端中存储的认证标识均为第一服务端生成的与该用户本次登陆时刻关联的认证标识，此时接入模块的比对结果为一致，允许通过第一服务端继续访问第二服务端。在本发明的一些实施方式中，对于 cognos 服务端(例如，一个或一个以上服务端)对应的服务器集群，可以是一台或一台以上计算机组成的计算机集群，接入模块在集群的内容管理主机(对于 cognos 系统，管理主机就是 Cognos content manager)上进行部署。一般而言，对于一个 Cognos 计算机集群来说，只有一个内容管理主机，也就是说，本发明实施方式中的接入模块可以只需部署在一个内容管理主机上即可。每次用户进行访问时，都可以调用内容管理主机上的接入模块进行对应的处理操作。需要说明的是，本领域技术人员可以根据 cognos 等报表应用对于认证的管理方式来确定接入模块的具体配置方式。

[0031] 本发明实施方式中，部署在第二服务端的接入模块在向第二服务端反馈认证通过，允许通过第一服务端继续访问第二服务端之后，还会对第一服务端在访问第二服务端时发送的认证信息进行验证，具体地，包括 :验证用户名是否正确，若该用户名正确，则查询该用户名对应的认证信息，所述认证信息包括用户名、该用户名所属机构和所属角色，具体而言，根据用户名到第一服务端的数据库中查询该用户名所属机构信息，并且根据用户名查询该用户名所属角色信息，并获取该用户名所属应用的所有机构以及该用户名所属应用的所有角色，并将验证通过后获取的信息(包括 :该用户名、该用户名所属机构和所属角色、和该用户名所属应用的所有机构和所有角色)组装为第二服务端可识别的 visa 对象。本发明实施方式中，用户名可认为是标识用户的标识 ID (例如，前述的 libin.xm)，用户名与其所属机构和所属角色关联，例如，用户名可以作为主键，该用户名所属机构和所属角色则可以作为该用户名对应主键的属性值。本发明实施方式中采用 visa 对象进行数据封装，提高了本发明中认证需求的应用范围。

[0032] 第二服务端在验证成功后，第二服务端(例如，Cognos 服务端)可以接收该用户名的访问请求，并根据 visa 对象分配给用户应具有的服务权限，进行相应的服务展现。在用户退出第二服务端后，第二服务端的数据库中除了全机构和全角色信息之外其他的信息(例如，登陆第一服务端生成的认证标识、该用户名所属机构和角色等信息)都可以随之删除。

[0033] 本发明实施方式中，接入模块通过 java 实施，编译后形成 jar 包，第二服务端支持调用 jar 包，同时也可以运行 jar 包，而接入模块与第一服务端之间通过 webservice 应用接口进行通信。

[0034] 以上结合实施例描述了本发明的认证接入方法，下面将结合实施例阐述采用上述认证接入方法的认证系统。

[0035] 参见图 2，图示了根据本发明实施方式的认证系统的示意图，该认证系统 200 包括第一服务端 201、与第一服务端连接的一个或一个以上第二服务端 202、部署在第一服务端

201 的生成模块 2010 和部署在第二服务端 202 的接入模块 2020，

[0036] 第一服务端 201，用于通过用户名登陆；

[0037] 所述生成模块 2010，用于在通过所述第一服务端的认证后，生成认证标识，其中所述认证标识与所述登陆第一服务端的时间相关联，并将所述用户名和所述认证标识写入所述第一服务端的数据库以及与所述第一服务端连接的一个或一个以上第二服务端的数据库；

[0038] 所述接入模块 2020，用于若通过所述第一服务端根据所述用户名访问所述第二服务端，根据所述用户名从所述第二服务端的数据库读取认证标识，并将所读取的认证标识与从所述第一服务端的数据库中读取的认证标识进行比对，若比对一致，则允许继续访问所述第二服务端。

[0039] 本发明实施方式中，用户通过用户名登陆第一服务端 201（例如，可以是中国建设银行开发的 RIDE 服务端），而第二服务端可以是各种行业领先的 BI 报表工具（例如，Cognos 服务端），作为前端的第一服务端（例如，RIDE 端）以作为后端的第二服务端为支撑。在一些特定实施方式中，企业资源管理系统、统计信息管理系统等等应用系统的报表展现功能不用进行单独开发，它们可以利用 RIDE+Cognos 的功能获得所有基本的报表展现服务。

[0040] 第一服务端和第二服务端之间通过 webservice 方式进行通讯，换而言之，第一服务端和第二服务端中的任意一个服务端通过调用另一个服务端提供的 webservice 接口来取得进入的入口方式。在同一应用服务中，第一服务端和第二服务端采用相同的认证方法，而对于不同的应用服务，基于认证安全的需要采用不同的认证方法。本发明提供的认证接入系统可以在不同应用服务（也就是对应不同认证方法）的场景下，无需对各个不同应用对应的不同认证方法单独进行认证配置，而是利用统一的认证标识进行认证处理，这种认证接入方式显著改善了认证处理的接入效率，特别在第二服务端个数较多（换而言之，对应应用服务数目较大）的场景中。

[0041] 在该用户名通过第一服务端的认证后，第一服务端记录该用户名的登陆状态为“已成功登陆”。在通过认证后，部署在第一服务端 201 的生成模块 2010 为该用户名生成认证标识，该认证标识与该用户名登陆第一服务端的时间相关联，也就是说，该认证标识随用户名登陆第一服务端的时间变化而变化，同一用户名在不同时间点登陆第一服务端所生成的认证标识不同。生成模块 2010 采用这种方式生成的认证标识可确保认证标识的实时性和唯一性，提高认证接入的安全性。在本发明的一些实施方式中，生成模块 2010 生成认证标识可以是与登陆第一服务端的时间相关联的字符串，例如，可以是 32 位的随机字符串。本领域技术人员可采用能实现上述目的的任何形式的认证标识，并不限于本文中提到的实施方式。

[0042] 生成模块 2010 在生成认证标识后，将用户本次登陆的用户名和该用户名本次登陆生成的认证标识一起写入第一服务端的数据库，同时写入与第一服务端连接的一个或一个以上（例如，两个、三个或更多个）第二服务端的数据库。本发明实施方式中的第二服务端可以是 Cognos、MSTR(Microstrategy)、BO（Business Object）等专业商务智能 BI 报表工具服务端。

[0043] 本发明实施方式中，在通过第一服务端认证之后，生成认证标识之前，还通过部署在第一服务端 201 的获取模块，从认证的数据库中获取该用户名所属机构和所属角色，以

及该用户名所属应用的所有机构和所有角色，并将该用户名、该用户名所属机构、该用户名所属角色组成认证信息，然后将组成的认证信息以及该用户名所属应用所有机构和所有角色写入第一服务端的数据库(例如，oracle 数据库)，以便后续管理用户对第一服务端进行权限管理。例如，对于银行目前使用的各种认证系统，一般要求用户具备所属机构和所属角色，以此来区分用户所应赋予的权限，以 libin.xm 为例，其所属机构可认为是“厦门分行”，所属角色为“会计部门一般查询人员”，则授予 libin.xm 的权限为查看厦门分行会计部的数据，而不能进行其他操作，如不能对所查看的数据变更修改，也不能查看此机构之外的数据。例如，某张报表“存款明细表”，在应用管理员对该报表授权时，第一服务端会将所有机构及所有角色列出，方便管理员从中选择出来进行授权(比如授予某个机构中的某个角色具有查看和删除该报表的权限)。其中，同一用户名以及该用户名所属机构和角色以一张数据库表的形式保存在数据库中，而该用户名所述应用的全机构、全角色各自以一张数据库表的形式进行存储。

[0044] 需要说明的是，当用户退出第一服务端后，除了该用户名所属应用的全机构、全角色之外的其他信息，例如本次登录生成的认证标识、该用户名所属机构和角色等都会删除，节省了存储空间，也有利于减低数据库中存在多个认证标识而导致的查询压力。

[0045] 若通过第一服务端 201 根据用户名访问第二服务端 202，配置在第二服务端 202 的接入模块 202 会根据访问第二服务端 202 的用户名从第二服务端数据库中查询该用户名对应的认证标识，并将从第二服务端数据库中读取的认证标识与从第一服务端数据库读取的认证标识进行比对，若比对一致，则可以通过向第二服务端反馈认证通过来允许继续访问第二服务端。在本发明的一些实施方式中，对于 cognos 服务端(例如，一个或一个以上服务端)对应的服务器集群，可以是一台或一台以上计算机组成的计算机集群，接入模块在集群的内容管理主机(对于 cognos 系统，管理主机就是 Cognos content manager)上进行部署。一般而言，对于一个 Cognos 计算机集群来说，只有一个内容管理主机，也就是说，本发明实施方式中的接入模块可以只需部署在一个内容管理主机上即可。每次用户进行访问时，都可以调用内容管理主机上的接入模块进行对应的处理操作。需要说明的是，本领域技术人员可以根据 cognos 等报表应用对于认证的管理方式来确定接入模块的具体配置方式。其中，本发明实施方式中的接入模块通 java 实施，编译后形成 jar 包，第二服务端支持调用并运行 jar 包。

[0046] 本发明实施方式中，配置在第二服务端的接入模块在向第二服务端反馈认证通过，允许通过第一服务端继续访问第二服务端之后，还会对第一服务端在访问第二服务端时发送的认证信息进行验证，具体地，包括 :验证用户名是否正确，若该用户名正确，则根据用户名查询该用户名对应的认证信息，所述认证信息包括该用户名、该用户名所属机构和所属角色，具体而言，根据用户名到第一服务端的数据库中查询该用户名所属机构信息，并且根据用户名查询该用户名所属角色信息，并获取该用户名所属应用的所有机构以及该用户名所属应用的所有角色，并将验证通过后获取的信息(包括 :该用户名、该用户名所属机构和所属角色、和该用户名所属应用的所有机构和所有角色)组装为第二服务端可识别的 visa 对象。本发明实施方式中，用户名可认为是标识用户的标识 ID (例如，前述的 libin.xm)，用户名与其所属机构和所属角色关联，例如，用户名可以作为主键，该用户名所属机构和所属角色则可以作为该用户名对应主键的属性值。本发明实施方式中采用 visa 对象进

行数据封装，提高了本发明中认证需求的应用范围。

[0047] 验证成功后，第二服务端 202（例如，Cognos 服务端）可以接收该用户名的访问请求，并根据 visa 对象分配给用户应具有的服务权限，进行相应的服务展现。在用户退出第二服务端后，第二服务端的数据库中除了全机构和全角色信息之外其他的信息（例如，登陆第一服务端生成的认证标识、该用户名所属机构和角色等信息）都可以随之删除。

[0048] 本发明实施方式中，配置在第二服务端的接入模块 2020 通过 webservice 应用接口与第一服务端 201 进行通信。

[0049] 综上所述，本发明的认证接入方法和认证系统，通过登录第一服务端后生成与登陆时间关联的一次性认证标识，并将生成的认证标识及用户名写入第一服务端和第二服务端的数据库，以便当通过第一服务端访问第二服务端时，通过部署在第二服务端的接入模块读取写入上述两服务端数据库的认证标识并进行比对，比对一致后可继续访问第二服务端，通过用户名结合唯一性认证标识的方式实现了在两种服务端之间的单点登陆；而且在认证标识比对通过后，将登陆第一服务端后获取的认证信息进行验证后封装为第二服务端可识别的 visa 对象进行权限分配，实现了不同认证方案场景下的集中认证，从整体上提高了认证系统的集成认证处理效率。

[0050] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明可借助软件结合硬件平台的方式来实现，当然也可以全部通过硬件来实施。基于这样的理解，本发明的技术方案对背景技术做出贡献的全部或者部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

[0051] 以上所揭露的仅为本发明的一种较佳实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

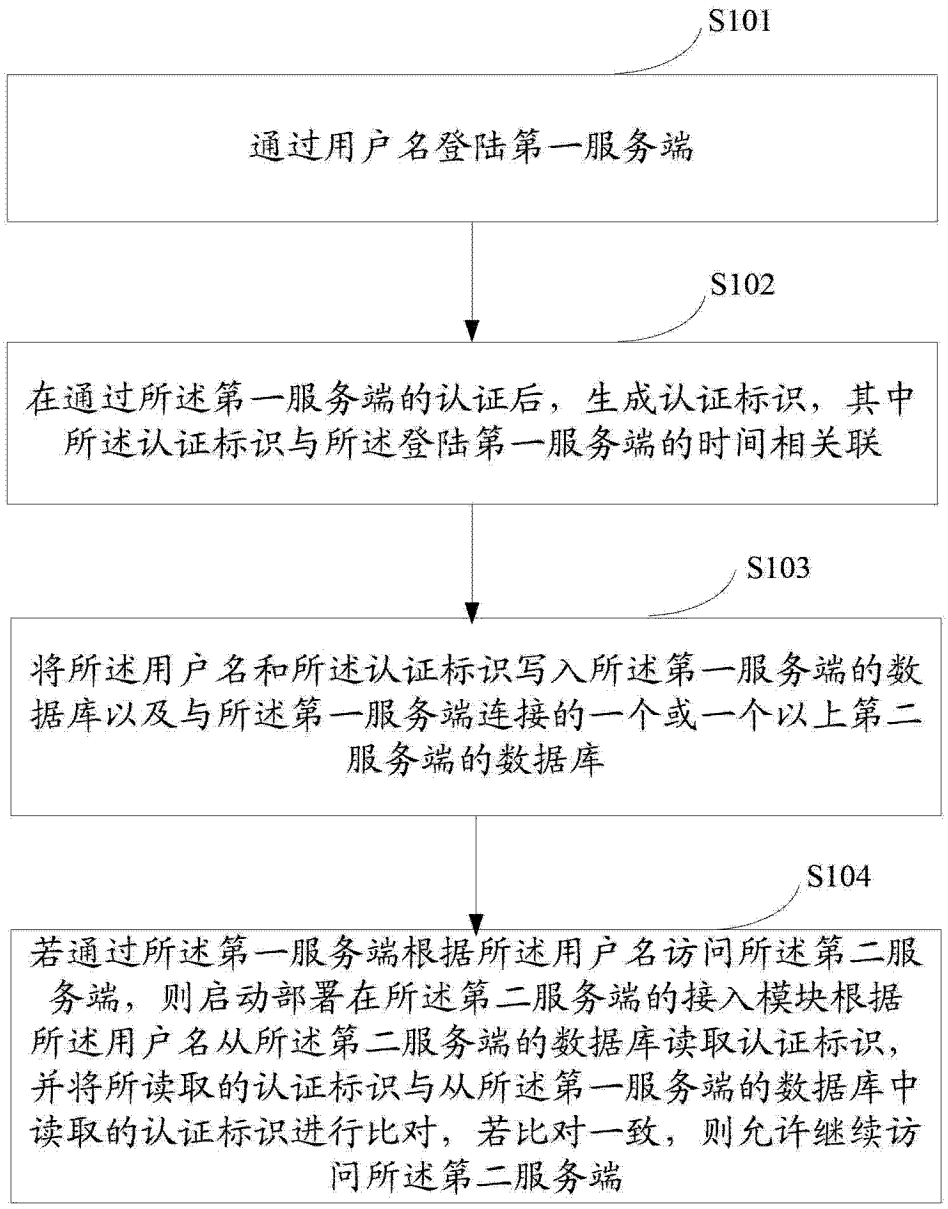

S101
通过用户名登陆第一服务端
S102
在通过所述第一服务端的认证后，生成认证标识，其中所述认证标识与所述登陆第一服务端的时间相关联
S103
将所述用户名和所述认证标识写入所述第一服务端的数据库以及与所述第一服务端连接的一个或一个以上第二服务端的数据库
S104
若通过所述第一服务端根据所述用户名访问所述第二服务端，则启动部署在所述第二服务端的接入模块根据所述用户名从所述第二服务端的数据库读取认证标识，并将所读取的认证标识与从所述第一服务端的数据库中读取的认证标识进行比对，若比对一致，则允许继续访问所述第二服务端

图 1

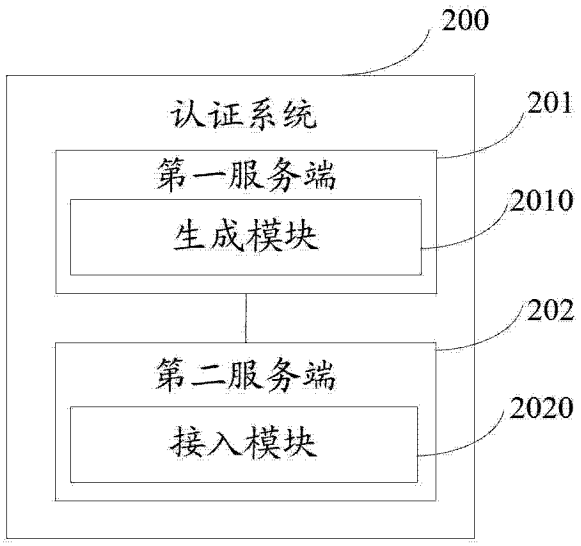


图 2