(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104769911 B
(45)授权公告日 2018.01.02

(21)申请号 201380057683.8
(22)申请日 2013.09.06
(65)同一申请的已公布的文献号
申请公布号 CN 104769911 A
(43)申请公布日 2015.07.08
(30)优先权数据
61/698,459 2012.09.07 US
61/698,463 2012.09.07 US
61/698,413 2012.09.07 US
61/785,299 2013.03.14 US
13/838,813 2013.03.15 US
(85)PCT国际申请进入国家阶段日
2015.05.05
(86)PCT国际申请的申请数据
PCT/US2013/058426 2013.09.06
(87)PCT国际申请的公布数据
WO2014/039772 EN 2014.03.13
(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 U·丝瑞尼瓦萨 V·阿索库玛
(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 李颖
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
US 2009265753 A1,2009.10.22,
EP 2458548 A1,2012.05.30,
CN 101202762 A,2008.06.18,
审查员 侯艳兰

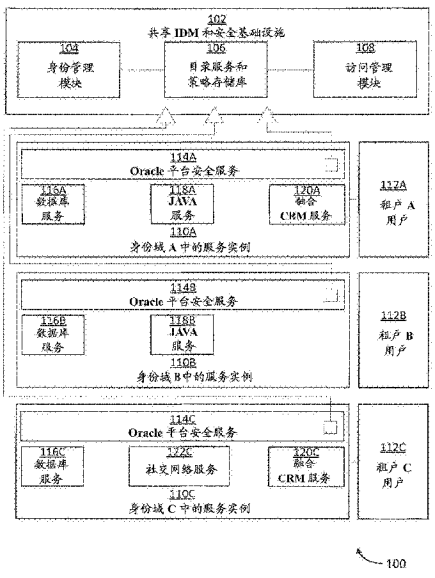
权利要求书10页 说明书44页 附图34页

(54)发明名称

多域身份管理系统

(57)摘要

多租户身份管理(IDM)系统使得能够对共享云计算环境内的各个不同客户的域实现IDM功能,而不为每个单独的域复制单独的IDM系统。在强制实施这些域之间的隔离的同时,IDM系统能够向位于各个不同客户的域内的服务实例提供IDM功能。整个云的身份存储库可包含多个客户的域的身份信息,整个云的策略存储库可包含多个客户的域的安全策略信息。多租户IDM系统可提供委托模型,在所述委托模型中,可为各个域指定域管理员,并且各个域管理员可把某些角色委派给属于他的域的其它用户身份。域管理员可以指定特定于服务实例的管理员,以管理域内的特定服务实例。



CN 104769911 B

1.一种计算机实现的方法,包括:

由共享身份管理系统创建与共享计算环境的多个客户中的第一客户相关的第一组用户身份,所述共享计算环境向与所述多个客户中的独立客户相关的用户提供服务;

把指定第一组用户身份并使第一组用户身份与第一客户相关的数据保存在共享计算环境中;

使共享计算环境内可用的第一批多个服务与第一客户关联;

根据第一批多个服务和第一客户之间的关联,由共享身份管理系统决定使第一批多个服务内的所有服务能够获得第一组用户身份;

由共享身份管理系统创建与多个客户中的第二客户相关的第二组用户身份;

把指定第二组用户身份并使第二组用户身份与第二客户相关的数据保存在共享计算环境中;

使共享计算环境内可用的第二批多个服务与第二客户关联;和

根据第二批多个服务和第二客户之间的关联,由共享身份管理系统决定使第二批多个服务内的所有服务能够获得第二组用户身份;

其中第一批多个服务不同于第二批多个服务;

其中共享身份管理系统为在专用于第一客户而不专用于第二客户的第一域内开通的服务提供身份管理功能;

其中共享身份管理系统为在专用于第二客户而不专用于第一客户的第二域内开通的服务提供身份管理功能;

其中第一域和第二域是共享计算环境的域。

2.按照权利要求1所述的计算机实现的方法,还包括:

通过共享身份管理系统,把(a)第一组用户身份中的第一用户映射到(b)对于第一批多个服务的子集的第一访问权限;

通过共享身份管理系统,把(c)第二组用户身份中的第二用户映射到(d)对于第二批多个服务的子集的第二访问权限;

其中第一组用户身份是作为第一客户的组织的雇员的一组身份;

其中第二组用户身份是作为第二客户的组织的雇员的一组身份。

3.按照权利要求1-2任意之一所述的计算机实现的方法,还包括:

通过共享身份管理系统,把(a)第一组用户身份中的第一用户映射到(b)第一角色,所述第一角色被映射到对于第一批多个服务的子集的第一访问权限;

通过共享身份管理系统,把(c)第二组用户身份中的第二用户映射到(d)第二角色,所述第二角色被映射到对于第二批多个服务的子集的第二访问权限。

4.按照权利要求1-2任意之一所述的计算机实现的方法,还包括:

阻止第一组用户身份中的用户进行与在第二组服务之中、但不在第一组服务之中的服务有关的操作;

阻止第二组用户身份中的用户进行与在第一组服务之中、但不在第二组服务之中的服务有关的操作。

5.按照权利要求1-2任意之一所述的计算机实现的方法,还包括:

把第一组用户身份的身份保存在由客户分隔的轻量存取协议LDAP目录的第一分区内;

和

把第二组用户身份的身份保存在LDAP目录的第二分区内。

6.按照权利要求1-2任意之一所述的计算机实现的方法，还包括：

呈现包括用户界面元素的用户界面，通过所述用户界面元素，作为登录过程的一部分，特定用户能够识别所述特定用户正在试图访问的共享计算环境的特定视图。

7.按照权利要求1-2任意之一所述的计算机实现的方法，还包括：

呈现控制台，所述控制台提供用于把用户身份增加到与多个客户中的特定客户相关的一组用户中，和从所述一组用户中删除用户身份的控件；

通过控制台，从身份域管理员接收命令；

确定身份域管理员属于的特定一组用户；和

把身份域管理员通过控制台进行的用户身份增加和删除操作局限于所述特定一组用户。

8.按照权利要求1-2任意之一所述的计算机实现的方法，还包括：

向第一组用户身份中的第一用户分配身份域管理员角色，所述身份域管理员角色给予第一用户向在第一组用户身份中具有身份的其他用户分配服务管理员角色的能力；

向由作为身份域管理员的第一用户选择的第一组用户身份中的第二用户，分配第一服务管理员角色，所述第一服务管理员角色给予第二用户管理第一批多个服务中的第一服务的能力；和

向由作为身份域管理员的第一用户选择的第一组用户身份中的第三用户，分配第二服务管理员角色，所述第二服务管理员角色给予第三用户管理第一批多个服务中的第二服务的能力。

9.按照权利要求1-2任意之一所述的计算机实现的方法，还包括：

从在第一组用户身份中无用户身份、但是与第一客户的账户相关的第一人，接收在第一组用户中也没有用户身份的第二人的电子邮件地址；

从所述第一人接收所述第一人提名第二人担任的角色；

向第二人的电子邮件地址发送电子邮件消息，所述电子邮件消息包含到基于web的表格的超链接，所述表格能够用于创建第一组用户身份内的用户身份；

根据第二人通过基于web的表格提供的信息，把第二人的身份增加到第一组用户身份；和

把所述角色分配给第二人的身份。

10.按照权利要求1-2任意之一所述的计算机实现的方法，还包括：

接收把特定服务增加到第一组服务中的请求；

响应所述请求，把所述特定服务增加到第一组服务中；和

在共享计算环境内，定义根据所述特定服务的类型，从角色的多个层次中自动选择的角色的层次。

11.按照权利要求1-2任意之一所述的计算机实现的方法，还包括：

将特定服务实例绑定到身份存储库的第一分区，所述特定服务实例是第一组服务中的服务的实例；和

将特定服务实例绑定到策略存储库的第二分区，所述策略存储库保存关于与多个客户

中的独立客户相关的多个服务实例的策略；

其中第一分区只包含与第一客户相关的身份；

其中第二分区只包含和特定服务实例有关的策略。

12.一种保存特定指令的计算机可读存储器，所述特定指令能够使一个或多个处理器进行指定操作，所述特定指令包括：

在共享计算环境内，创建多个客户-服务关联和多个客户-用户关联的指令，所述共享计算环境向与共享计算环境的多个客户中的独立客户相关的用户提供服务；

根据客户-服务关联和客户-用户关联，对于共享计算环境的多个用户中的每个特定用户，确定所述特定用户被准许访问的服务的子集的指令；

把服务实例增加到所述多个客户-服务关联中的特定客户-服务关联中的指令；

保存使服务实例和身份存储库的特定分区相关联的数据的指令，所述身份存储库保存每个客户-用户关联中的用户的身份；

保存使服务实例和策略存储库的特定分区相关联的数据的指令，所述策略存储库保存关于每个客户-服务关联中的服务实例的策略；和

提供共享身份管理系统的指令，所述共享身份管理系统为在专用于多个客户中的第一客户而不专用于多个客户中的第二客户的第一域内开通的服务提供身份管理功能；

其中共享身份管理系统为在专用于第二客户而不专用于第一客户的第二域内开通的服务提供身份管理功能；

其中第一域和第二域是共享计算环境的域。

13.按照权利要求12所述的计算机可读存储器，其中所述特定指令还包括：

把角色的层次中的第一角色分配给第一用户的指令，所述第一用户具有保存在身份存储库中并在特定的客户-用户关联中指定的第一用户身份；

其中第一角色是允许具有第一角色的用户管理在所述特定客户-服务关联中指定的所有服务实例的角色；

把所述角色的层次中的第二角色分配给第二用户的指令，所述第二用户具有保存在身份存储库中的第二用户身份；

其中第二角色是允许具有第二角色的用户管理在特定的客户-服务关联中指定的单一服务实例的角色。

14.按照权利要求13所述的计算机可读存储器，其中把第二角色分配给第二用户的指令包括响应于第一用户把第二角色委派给第二用户，把第二角色分配给第二用户的指令。

15.按照权利要求13所述的计算机可读存储器，其中增加服务实例的指令包括向第三用户分配第三角色的指令，所述第三用户具有保存在身份存储库中并且在特定的客户-用户关联内指定的第三身份，所述第三角色由与特定服务实例的类型相关的多个角色定义。

16.按照权利要求15所述的计算机可读存储器，其中所述特定指令包括使第二角色继承与第三角色相关的所有权限的指令；其中所述特定指令包括使第一角色继承被第二角色继承的所有权限的指令。

17.按照权利要求12所述的计算机可读存储器，其中所述特定指令还包括向指定的电子邮件地址发送电子邮件消息的指令，所述电子邮件消息提供一种机制，借助所述机制，电子邮件消息的收件人能够在特定的客户-用户关联内建立管理身份。

18.一种方法,包括:

导致在共享计算环境中建立单一身份管理IDM系统,所述共享计算环境向与共享计算环境的多个客户中的独立客户相关的用户提供服务;

使所述单一IDM系统向与共享计算环境的第一客户相关的第一服务实例提供IDM功能;

使所述单一IDM系统向与共享计算环境的第二客户相关的第二服务实例提供IDM功能;

使所述单一IDM系统阻止与第一客户相关的用户访问第二服务实例;和

使所述单一IDM系统阻止与第二客户相关的用户访问第一服务实例;

其中单一IDM系统为在专用于第一客户而不专用于第二客户的第一域内开通的服务提供身份管理功能;

其中单一IDM系统为在专用于第二客户而不专用于第一客户的第二域内开通的服务提供身份管理功能;

其中第一域和第二域是共享计算环境的域。

19.按照权利要求18所述的方法,还包括:

使所述单一IDM系统把与第一客户相关、但是不与第二客户相关的用户身份保存在维持于共享计算环境内的单一身份存储库内;

使所述单一IDM系统把与第二客户相关、但是不与第一客户相关的用户身份保存在所述单一身份存储库内;

使所述单一IDM系统生成第一凭证,所述第一凭证允许第一服务实例与所述单一身份存储库的包含和第一客户相关的用户身份的一部分交互作用,但不允许第一服务实例与所述单一身份存储库的包含和第一客户不相关的用户身份的各个部分交互作用;和

使所述单一IDM系统生成第二凭证,所述第二凭证允许第二服务实例与所述单一身份存储库的包含和第二客户相关的用户身份的一部分交互作用,但不允许第二服务实例与所述单一身份存储库的包含和第二客户不相关的用户身份的各个部分交互作用。

20.按照权利要求18所述的方法,还包括:

使所述单一IDM系统把与第一服务实例相关、但是不与第二服务实例相关的安全访问策略保存在维持于共享计算环境内的单一策略存储库内;

使所述单一IDM系统把与第二服务实例相关、但是不与第一服务实例相关的安全访问策略保存在所述单一策略存储库内;

使所述单一IDM系统生成第一凭证,所述第一凭证允许第一服务实例与所述单一策略存储库的包含和第一服务实例相关的安全访问策略的一部分交互作用,但不允许第一服务实例与所述单一策略存储库的包含和第一服务实例不相关的安全访问策略的各个部分交互作用;和

使所述单一IDM系统生成第二凭证,所述第二凭证允许第二服务实例与所述单一策略存储库的包含和第二服务实例相关的安全访问策略的一部分交互作用,但不允许第二服务实例与所述单一策略存储库的包含和第二服务实例不相关的安全访问策略的各个部分交互作用。

21.一种系统,包括:

由共享身份管理系统创建与共享计算环境的多个客户中的第一客户相关的第一组用户身份的装置,所述共享计算环境向与所述多个客户中的独立客户相关的用户提供服务;

把指定第一组用户身份并使第一组用户身份与第一客户相关的数据保存在共享计算环境中的装置；

使共享计算环境内可用的第一批多个服务与第一客户关联的装置；

根据第一批多个服务和第一客户之间的关联，由共享身份管理系统决定使第一批多个服务内的所有服务能够获得第一组用户身份的装置；

由共享身份管理系统创建与多个客户中的第二客户相关的第二组用户身份的装置；

把指定第二组用户身份并使第二组用户身份与第二客户相关的数据保存在共享计算环境中的装置；

使共享计算环境内可用的第二批多个服务与第二客户关联的装置；和

根据第二批多个服务和第二客户之间的关联，由共享身份管理系统决定使第二批多个服务内的所有服务能够获得第二组用户身份的装置；

其中第一批多个服务不同于第二批多个服务；

其中共享身份管理系统为在专用于第一客户而不专用于第二客户的第一域内开通的服务提供身份管理功能；

其中共享身份管理系统为在专用于第二客户而不专用于第一客户的第二域内开通的服务提供身份管理功能；

其中第一域和第二域是共享计算环境的域。

22.按照权利要求21所述的系统，还包括：

通过共享身份管理系统，把(a)第一组用户身份中的第一用户映射到(b)对于第一批多个服务的子集的第一访问权限的装置；

通过共享身份管理系统，把(c)第二组用户身份中的第二用户映射到(d)对于第二批多个服务的子集的第二访问权限的装置；

其中第一组用户身份是作为第一客户的组织的雇员的一组身份；

其中第二组用户身份是作为第二客户的组织的雇员的一组身份。

23.按照权利要求21-22任意之一所述的系统，还包括：

通过共享身份管理系统，把(a)第一组用户身份中的第一用户映射到(b)第一角色的装置，所述第一角色被映射到对于第一批多个服务的子集的第一访问权限；

通过共享身份管理系统，把(c)第二组用户身份中的第二用户映射到(d)第二角色的装置，所述第二角色被映射到对于第二批多个服务的子集的第二访问权限。

24.按照权利要求21-22任意之一所述的系统，还包括：

阻止第一组用户身份中的用户进行与在第二组服务之中、但不在第一组服务之中的服务有关的操作的装置；

阻止第二组用户身份中的用户进行与在第一组服务之中、但不在第二组服务之中的服务有关的操作的装置。

25.按照权利要求21-22任意之一所述的系统，还包括：

把第一组用户身份的身份保存在由客户分隔的轻量存取协议LDAP目录的第一分区内的装置；和

把第二组用户身份的身份保存在LDAP目录的第二分区内的装置。

26.按照权利要求21-22任意之一所述的系统，还包括：

呈现包括用户界面元素的用户界面的装置，通过所述用户界面元素，作为登录过程的一部分，特定用户能够识别所述特定用户正在试图访问的共享计算环境的特定视图。

27.按照权利要求21-22任意之一所述的系统，还包括：

呈现控制台的装置，所述控制台提供用于把用户身份增加到与多个客户中的特定客户相关的一组用户中，和从所述一组用户中删除用户身份的控件；

通过控制台，从身份域管理员接收命令的装置；

确定身份域管理员属于的特定一组用户的装置；和

把身份域管理员通过控制台进行的用户身份增加和删除操作局限于所述特定一组用户的装置。

28.按照权利要求21-22任意之一所述的系统，还包括：

向第一组用户身份中的第一用户分配身份域管理员角色的装置，所述身份域管理员角色给予第一用户向在第一组用户身份中具有身份的其他用户分配服务管理员角色的能力；

向由作为身份域管理员的第一用户选择的第一组用户身份中的第二用户，分配第一服务管理员角色的装置，所述第一服务管理员角色给予第二用户管理第一批多个服务中的第一服务的能力；和

向由作为身份域管理员的第一用户选择的第一组用户中身份的第三用户，分配第二服务管理员角色的装置，所述第二服务管理员角色给予第三用户管理第一批多个服务中的第二服务的能力。

29.按照权利要求21-22任意之一所述的系统，还包括：

从在第一组用户身份中无用户身份、但是与第一客户的账户相关的第一人，接收在第一组用户中也没有用户身份的第二人的电子邮件地址的装置；

从所述第一人接收所述第一人提名第二人担任的角色的装置；

向第二人的电子邮件地址发送电子邮件消息的装置，所述电子邮件消息包含到基于web的表格的超链接，所述表格能够用于创建第一组用户身份内的用户身份；

根据第二人通过基于web的表格提供的信息，把第二人的身份增加到第一组用户身份的装置；和

把所述角色分配给第二人的身份的装置。

30.按照权利要求21-22任意之一所述的系统，还包括：

接收把特定服务增加到第一组服务中的请求的装置；

响应所述请求，把所述特定服务增加到第一组服务中的装置；和

在共享计算环境内，定义根据所述特定服务的类型，从角色的多个层次中自动选择的角色的层次的装置。

31.按照权利要求21-22任意之一所述的系统，还包括：

将特定服务实例绑定到身份存储库的第一分区的装置，所述特定服务实例是第一组服务中的服务的实例；和

将特定服务实例绑定到策略存储库的第二分区的装置，所述策略存储库保存关于与多个客户中的独立客户相关的多个服务实例的策略；

其中第一分区只包含与第一客户相关的身份；

其中第二分区只包含和特定服务实例有关的策略。

32.一种系统,包括:

在共享计算环境内,创建多个客户-服务关联和多个客户-用户关联的装置,所述共享计算环境向与共享计算环境的多个客户中的独立客户相关的用户提供服务;

根据客户-服务关联和客户-用户关联,对于共享计算环境的多个用户中的每个特定用户,确定所述特定用户被准许访问的服务的子集的装置;

把服务实例增加到所述多个客户-服务关联中的特定客户-服务关联中的装置;

保存使服务实例和身份存储库的特定分区相关联的数据的装置,所述身份存储库保存每个客户-用户关联中的用户的身份;

保存使服务实例和策略存储库的特定分区相关联的数据的装置,所述策略存储库保存关于每个客户-服务关联中的服务实例的策略;和

提供共享身份管理系统的装置,所述共享身份管理系统为在专用于多个客户中的第一客户而不专用于多个客户中的第二客户的第一域内开通的服务提供身份管理功能;

其中共享身份管理系统为在专用于第二客户而不专用于第一客户的第二域内开通的服务提供身份管理功能;

其中第一域和第二域是共享计算环境的域。

33.按照权利要求32所述的系统,还包括:

把角色的层次中的第一角色分配给第一用户的装置,所述第一用户具有保存在身份存储库中并在特定的客户-用户关联中指定的第一用户身份;

其中第一角色是允许具有第一角色的用户管理在所述特定客户-服务关联中指定的所有服务实例的角色;

把所述角色的层次中的第二角色分配给第二用户的装置,所述第二用户具有保存在身份存储库中的第二用户身份;

其中第二角色是允许具有第二角色的用户管理在特定的客户-服务关联中指定的单一服务实例的角色。

34.按照权利要求33所述的系统,其中把第二角色分配给第二用户的装置包括响应于第一用户把第二角色委派给第二用户,把第二角色分配给第二用户的装置。

35.按照权利要求33或34所述的系统,其中增加服务实例的装置包括向第三用户分配第三角色的装置,所述第三用户具有保存在身份存储库中并且在特定的客户-用户关联内指定的第三身份,所述第三角色由与特定服务实例的类型相关的多个角色定义。

36.按照权利要求35所述的系统,还包括:使第二角色继承与第三角色相关的所有权限的装置;和使第一角色继承被第二角色继承的所有权限的装置。

37.按照权利要求32-34任意之一所述的系统,还包括向指定的电子邮件地址发送电子邮件消息的装置,所述电子邮件消息提供一种机制,借助所述机制,电子邮件消息的收件人能够在特定的客户-用户关联内建立管理身份。

38.一种包括云计算环境内的单一身份管理IDM的系统,包括:

向与共享计算环境的第一客户相关的第一服务实例提供IDM功能的装置;

向与共享计算环境的第二客户相关的第二服务实例提供IDM功能的装置;

阻止与第一客户相关的用户访问第二服务实例的装置;和

阻止与第二客户相关的用户访问第一服务实例的装置;

其中向第一服务实例提供IDM功能的装置是用于向第二服务实例提供IDM功能的装置；

其中向第一服务实例提供IDM功能的装置为在专用于第一客户而不专用于第二客户的第一域内开通的服务提供身份管理功能；

其中向第二服务实例提供IDM功能的装置为在专用于第二客户而不专用于第一客户的第二域内开通的服务提供身份管理功能；

其中第一域和第二域是共享计算环境的域。

39.按照权利要求38所述的系统，还包括：

把与第一客户相关、但是不与第二客户相关的用户身份保存在维持于共享计算环境内的单一身份存储库内的装置；

把与第二客户相关、但是不与第一客户相关的用户身份保存在所述单一身份存储库内的装置；

生成第一凭证的装置，所述第一凭证允许第一服务实例与所述单一身份存储库的包含和第一客户相关的用户身份的一部分交互作用，但不允许第一服务实例与所述单一身份存储库的包含和第一客户不相关的用户身份的各个部分交互作用；和

生成第二凭证的装置，所述第二凭证允许第二服务实例与所述单一身份存储库的包含和第二客户相关的用户身份的一部分交互作用，但不允许第二服务实例与所述单一身份存储库的包含和第二客户不相关的用户身份的各个部分交互作用。

40.按照权利要求38或39所述的系统，还包括：

把与第一服务实例相关、但是不与第二服务实例相关的安全访问策略保存在维持于共享计算环境内的单一策略存储库内的装置；

把与第二服务实例相关、但是不与第一服务实例相关的安全访问策略保存在所述单一策略存储库内的装置；

生成第一凭证的装置，所述第一凭证允许第一服务实例与所述单一策略存储库的包含和第一服务实例相关的安全访问策略的一部分交互作用，但不允许第一服务实例与所述单一策略存储库的包含和第一服务实例不相关的安全访问策略的各个部分交互作用；和

生成第二凭证的装置，所述第二凭证允许第二服务实例与所述单一策略存储库的包含和第二服务实例相关的安全访问策略的一部分交互作用，但不允许第二服务实例与所述单一策略存储库的包含和第二服务实例不相关的安全访问策略的各个部分交互作用。

41.一种方法，包括：

在共享计算环境内，创建多个客户-服务关联和多个客户-用户关联，所述共享计算环境向与共享计算环境的多个客户中的独立客户相关的用户提供服务；

根据客户-服务关联和客户-用户关联，对于共享计算环境的多个用户中的每个特定用户，确定所述特定用户被准许访问的服务的子集；

把服务实例增加到所述多个客户-服务关联中的特定客户-服务关联中；

保存使服务实例和身份存储库的特定分区相关联的数据，所述身份存储库保存每个客户-用户关联中的用户的身份；

保存使服务实例和策略存储库的特定分区相关联的数据，所述策略存储库保存关于每个客户-服务关联中的服务实例的策略；和

提供共享身份管理系统，所述共享身份管理系统为在专用于多个客户中的第一客户而

不专用于多个客户中的第二客户的第一域内开通的服务提供身份管理功能；

其中共享身份管理系统为在专用于第二客户而不专用于第一客户的第二域内开通的服务提供身份管理功能；

其中第一域和第二域是共享计算环境的域。

42.按照权利要求41所述的方法，还包括：

把角色的层次中的第一角色分配给第一用户，所述第一用户具有保存在身份存储库中并在特定的客户-用户关联中指定的第一用户身份；

其中第一角色是允许具有第一角色的用户管理在所述特定客户-服务关联中指定的所有服务实例的角色；

把所述角色的层次中的第二角色分配给第二用户，所述第二用户具有保存在身份存储库中的第二用户身份；

其中第二角色是允许具有第二角色的用户管理在特定的客户-服务关联中指定的单一服务实例的角色。

43.按照权利要求41或42所述的方法，还包括响应于第一用户把第二角色委派给第二用户，把第二角色分配给第二用户。

44.按照权利要求43所述的方法，还包括向第三用户分配第三角色，所述第三用户具有保存在身份存储库中并且在特定的客户-用户关联中指定的第三身份，所述第三角色由与特定服务实例的类型相关的多个角色定义。

45.按照权利要求44所述的方法，还包括使第二角色继承与第三角色相关的所有权限；以及使计算机使得第一角色继承被第二角色继承的所有权限。

46.按照权利要求41-42任意之一所述的方法，还包括向指定的电子邮件地址发送电子邮件消息，所述电子邮件消息提供一种机制，借助所述机制，电子邮件消息的收件人能够在所述特定客户-用户关联内建立管理身份。

47.一种系统，包括：

一个或多个处理器，所述处理器被配置为：

导致在共享计算环境中，建立单一身份管理IDM系统，所述共享计算环境向与共享计算环境的多个客户中的独立客户相关的用户提供服务；

使所述单一IDM系统向与共享计算环境的第一客户相关的第一服务实例提供IDM功能；

使所述单一IDM系统向与共享计算环境的第二客户相关的第二服务实例提供IDM功能；

使所述单一IDM系统阻止与第一客户相关的用户访问第二服务实例；和

使所述单一IDM系统阻止与第二客户相关的用户访问第一服务实例；

其中单一IDM系统为在专用于第一客户而不专用于第二客户的第一域内开通的服务提供身份管理功能；

其中单一IDM系统为在专用于第二客户而不专用于第一客户的第二域内开通的服务提供身份管理功能；

其中第一域和第二域是共享计算环境的域。

48.按照权利要求47所述的系统，其中所述处理器还被配置为：

使所述单一IDM系统把与第一客户相关、但是不与第二客户相关的用户身份保存在维持于共享计算环境内的单一身份存储库内；

使所述单一IDM系统把与第二客户相关、但是不与第一客户相关的用户身份保存在所述单一身份存储库内；

使所述单一IDM系统生成第一凭证，所述第一凭证允许第一服务实例与所述单一身份存储库的包含和第一客户相关的用户身份的一部分交互作用，但不允许第一服务实例与所述单一身份存储库的包含和第一客户不相关的用户身份的各个部分交互作用；和

使所述单一IDM系统生成第二凭证，所述第二凭证允许第二服务实例与所述单一身份存储库的包含和第二客户相关的用户身份的一部分交互作用，但不允许第二服务实例与所述单一身份存储库的包含和第二客户不相关的用户身份的各个部分交互作用。

49.按照权利要求47或48所述的系统，其中所述处理器还被配置为：

使所述单一IDM系统把与第一服务实例相关、但是不与第二服务实例相关的安全访问策略保存在维持于共享计算环境内的单一策略存储库内；

使所述单一IDM系统把与第二服务实例相关、但是不与第一服务实例相关的安全访问策略保存在所述单一策略存储库内；

使所述单一IDM系统生成第一凭证，所述第一凭证允许第一服务实例与所述单一策略存储库的包含和第一服务实例相关的安全访问策略的一部分交互作用，但不允许第一服务实例与所述单一策略存储库的包含和第一服务实例不相关的安全访问策略的各个部分交互作用；和

使所述单一IDM系统生成第二凭证，所述第二凭证允许第二服务实例与所述单一策略存储库的包含和第二服务实例相关的安全访问策略的一部分交互作用，但不允许第二服务实例与所述单一策略存储库的包含和第二服务实例不相关的安全访问策略的各个部分交互作用。

多域身份管理系统

[0001] 相关申请的引用

[0002] 本申请要求以下申请的优先权:2013年3月13日提交的美国专利申请No.13/838,813,“MULTI-TENANCY IDENTITY MANAGEMENT SYSTEM”,其所有内容通过引用包含于此;2012年9月7日提交的美国临时专利申请No.61/698,463,“SHARED IDENTITY MANAGEMENT ARCHITECTURE”,其所有内容通过引用包含于此;2012年9月7日提交的美国临时专利申请No.61/698,413,“TENANT AUTOMATION SYSTEM”,其所有内容通过引用包含于此;2012年9月7日提交的美国临时专利申请No.61/698,459,“SERVICE DEPLOYMENT INFRASTRUCTURE”;和2014年3月14日提交的美国临时专利申请No.61/785,299,“CLOUD INFRASTRUCTURE”,其所有内容通过引用包含于此。

技术领域

[0003] 本公开涉及计算机安全,更具体地,涉及被分成各个单独的身份域的云计算环境内的身份管理。

背景技术

[0004] 云计算涉及通过网络(一般是因特网),以服务的形式交付的计算资源(例如,硬件和软件)的使用。云计算把用户的数据、软件和计算委托给远程服务。例如,云计算可用于提供软件即服务(SaaS)或平台即服务(PaaS)。在利用SaaS的业务模型中,可向用户提供对应用软件和数据库的访问。云提供者可管理应用运行于的基础设施和平台。SaaS提供者通常利用预订费,给应用定价。SaaS可使企业获得通过把硬件和软件维护和支持外包给云提供者,来降低信息技术运营成本的潜能。这种外包可使企业能够远离硬件/软件开销和人员费用地重新分配信息技术运营费用,以满足其它信息技术目标。此外,由于应用被集中托管,因此能够不需要用户安装新软件地发布更新。然而,由于用户的数据被保存在云提供者的服务器上,因此,一些机构担心可能的对所述数据的潜在访问。

[0005] 通过web浏览器或者轻型桌面或移动应用,最终用户能够访问基于云的应用。同时,企业软件和用户的数据可被保存在位于远离所述企业和用户的位置的服务器上。至少在理论上,云计算使企业可以更迅速地部署其应用,同时可管理性得到改善,并且维护更少。至少在理论上,云计算使信息技术管理者可以更快地调整资源,以满足不时波动和不可预测的企业需求。

[0006] 身份管理(IDM)是控制计算机系统的用户的有关信息的任务。所述信息可包括验证所述用户的身份的信息。所述信息可包括描述所述用户被准许访问哪些数据的信息。所述信息可包括描述所述用户被准许对各种系统资源(例如,文件、目录、应用、通信端口、存储段等),进行哪些操作的信息。IDM还可包括关于各个用户的描述信息以及所述描述信息可被谁如何访问和变更的管理。

[0007] 潜在地,云计算环境可包括用于使用云计算环境的各个独立机构的独立IDM系统,或者IDM系统的独立实例。不过,这种方案被视为工作的重复,和计算资源的浪费。

发明内容

[0008] 本发明的一些实施例涉及在云计算环境中实现的、被分成多个单独的身份域的身份管理(IDM)系统。

[0009] 在本发明的实施例中，一组构成都排列在一起，从而创建单一IDM系统的抽象或者“租户切片化”视图。所述单一IDM系统可包括多个独立的组件或子系统。IDM系统可在多个独立的单独“租户”或者说IDM系统客户之间被共享，以致IDM系统被更密集地使用。从而，不需要为每个单独的客户例示单独的IDM系统。所述单一IDM系统可被配置成以致对于IDM系统的各个租户，可向该租户的用户呈现特定于该租户的IDM系统的虚拟视图。

[0010] 本发明的实施例可以利用虚拟化的概念。可按照概念上和在单一的主计算设备上可虚拟化多个单独虚拟机的方式类似的方式，在所述单一IDM系统内虚拟化IDM系统的单独视图。通过按照特定的方式配置IDM系统，可以实现这种虚拟化。IDM系统可涉及多个单独的层，包括概念上一个垂直地堆叠在另一个之上的上层和下层。上层至少可被分区。在IDM系统中，各个不同的服务(例如，验证和/或授权服务)可以与IDM系统的各个不同租户关联。IDM系统可以隔离各个租户，以致各个租户只能够与专用于该租户的IDM系统“切片”或分区交互作用。从而，IDM系统可强制实施租户之间的隔离。

[0011] 本发明的例证实施例提供一种计算机实现的方法，包括：在云计算环境内，创建多个身份域；在所述多个身份域内，强制实施身份域之间的隔离；把服务实例增加到所述多个身份域中的特定身份域；保存使服务实例和身份存储库的特定分区关联的数据，所述身份存储库保存所述多个身份域中的每个身份域的身份；和保存使服务实例和策略存储库的特定分区相关联的数据，所述策略存储库保存关于与所述多个身份域中的不同身份域相关的多个服务实例的策略。

[0012] 在例子中，计算机实现的方法还包括：把角色的层次中的第一角色分配给第一用户，所述第一用户具有保存在身份存储库中并且与特定身份域相关的第一用户身份，其中第一角色是允许具有第一角色的用户管理与所述特定身份域相关的所有服务实例的角色；把所述角色的层次中的第二角色分配给第二用户，所述第二用户具有保存在身份存储库中的第二用户身份，其中第二角色是允许具有第二角色的用户管理与所述特定身份域相关的单一服务实例的角色。

[0013] 在例子中，把第二角色分配给第二用户包括响应第一用户把第二角色委派给第二用户，把第二角色分配给第二用户。

[0014] 在例子中，把服务实例增加到所述多个身份域中的特定身份域中包括向第三用户分配第三角色，所述第三用户具有保存在身份存储库中并且与所述特定身份域相关的第三身份，所述第三角色由与特定服务实例的类型相关的多个角色定义。

[0015] 在例子中，计算机实现的方法还包括：使第二角色继承与第三角色相关的所有权限(permission)；和使第一角色继承被第二角色继承的所有权限。

[0016] 在例子中，在云计算环境内创建多个身份域包括在云计算环境内创建所述特定身份域，在云计算环境内创建所述特定身份域包括向指定的电子邮件地址发送电子邮件消息，所述电子邮件消息提供一种机制，借助所述机制，电子邮件消息的收件人能够在所述特定身份域内，建立管理身份。

[0017] 本发明的例证实施例提供一种计算机实现的方法，包括：导致在云计算环境中建立单一身份管理(IDM)系统；使所述单一IDM系统向与第一身份域相关的第一服务实例提供IDM功能，所述第一身份域是在云计算环境内定义的并且与在云计算环境内定义的第二身份域隔离；和使所述单一IDM系统向与第二身份域相关的第二服务实例提供IDM功能。

[0018] 在例子中，计算机实现的方法还包括：使所述单一IDM系统把与第一身份域相关、但是不与第二身份域相关的用户身份保存在维持于云计算环境内的单一身份存储库内；使所述单一IDM系统把与第二身份域相关、但是不与第一身份域相关的用户身份保存在所述单一身份存储库内；使所述单一IDM系统生成第一凭证，所述第一凭证允许第一服务实例与所述单一身份存储库的包含和第一身份域相关的用户身份的一部分交互作用，但不允许第一服务实例与所述单一身份存储库的包含和第一身份域不相关的用户身份的各个部分交互作用；和使所述单一IDM系统生成第二凭证，所述第二凭证允许第二服务实例与所述单一身份存储库的包含和第二身份域相关的用户身份的一部分交互作用，但不允许第二服务实例与所述单一身份存储库的包含和第二身份域不相关的用户身份的各个部分交互作用。

[0019] 在例子中，计算机实现的方法还包括：使所述单一IDM系统把与第一服务实例相关、但是不与第二服务实例相关的安全访问策略保存在维持于云计算环境内的单一策略存储库内；使所述单一IDM系统把与第二服务实例相关，但是不与第一服务实例相关的安全访问策略保存在所述单一策略存储库内；使所述单一IDM系统生成第一凭证，所述第一凭证允许第一服务实例与所述单一策略存储库的包含和第一服务实例相关的安全访问策略的一部分交互作用，但不允许第一服务实例与所述单一策略存储库的包含和第一服务实例不相关的安全访问策略的各个部分交互作用；和使所述单一IDM系统生成第二凭证，所述第二凭证允许第二服务实例与所述单一策略存储库的包含和第二服务实例相关的安全访问策略的一部分交互作用，但不允许第二服务实例与所述单一策略存储库的包含和第二服务实例不相关的安全访问策略的各个部分交互作用。

附图说明

[0020] 图1是按照本发明的实施例，从租户的角度图解说明共享IDM系统的例子的方框图；

[0021] 图2是按照本发明的实施例，图解说明通过共享IDM系统，为多个客户创建多个身份域的技术的例子的流程图；

[0022] 图3是按照本发明的实施例，图解说明分层的云基IDM系统的概况的例子的方框图；

[0023] 图4是按照本发明的实施例，图解说明云安全基础层的子系统的例子的方框图；

[0024] 图5是按照本发明的实施例，图解说明云共享IDM层的子系统的例子的方框图；

[0025] 图6是按照本发明的实施例，图解说明Oracle IDM/安全层的子系统的例子的方框图；

[0026] 图7是按照本发明的实施例，图解说明其中角色层次可用于管理身份域的云基IDM系统的例子的方框图；

[0027] 图8是按照本发明的实施例，图解说明其中使应用实例运行时组件可访问在身份域内定义的身份的多租户IDM系统的方框图；

[0028] 图9是图解说明按照本发明的实施例可使用的系统环境的组件的简化方框图；

[0029] 图10是按照本发明的实施例可使用的计算机系统的简化方框图；

[0030] 图11是按照本发明的实施例，图解说明多租户IDM系统中的角色授权的方框图；

[0031] 图12是按照本发明的实施例，图解说明多租户IDM系统中的权限继承的方框图；

[0032] 图13是按照本发明的实施例，图解说明提供身份域内的服务实例的系统的例子的方框图；

[0033] 图14是按照本发明的实施例，图解说明其中可在身份域之间，共享云的硬件和软件资源的多租户云基系统的例子的方框图；

[0034] 图15是按照本发明的实施例，图解说明可在云基系统中，用于在隔离的客户之间，共享云硬件的虚拟“切片”的JAVA云服务体系结构的例子的方框图；

[0035] 图16是按照本发明的实施例，图解说明云基IDM系统的多租户LDAP目录的结构的例子的分层示图；

[0036] 图17是按照本发明的实施例，图解说明与用于不同服务类型的角色模板有关的LDAP目录子树的结构的例子的分层示图；

[0037] 图18是按照本发明的实施例，图解说明可用在云基系统中，并且其中在相同数据库实例中，可以使用多种模式的数据库云服务多租户体系结构的例子的方框图；

[0038] 图19是按照本发明的实施例，图解说明Nuviaq云系统的例子的方框图；

[0039] 图20A是按照本发明的一个实施例的云基础设施系统的逻辑视图；

[0040] 图20B是可用于实现按照本发明的实施例的云基础设施系统的硬件/软件栈的简化方框图；

[0041] 图21是实现图20A中所示的云基础设施系统的系统环境的简化方框图；

[0042] 图22A是按照本发明的实施例，说明由云基础设施系统中的TAS模块进行的处理的简化流程图；

[0043] 图22B是按照本发明的实施例，说明云基础设施系统中的TAS模块中的一个或多个子模块的简化高级示图；

[0044] 图23按照本发明的实施例，说明TAS组件的例证分布式部署；

[0045] 图24是按照本发明的实施例，图解说明SDI模块与云基础设施系统中的一个或多个模块的交互作用的简化方框图；

[0046] 图25是按照本发明的实施例的SDI模块的子模块的简化高级示图；

[0047] 图26A是按照本发明的实施例，说明由云基础设施系统中的SDI组件进行的处理的简化流程图；

[0048] 图26B是按照本发明的实施例，表示Nuviaq系统的高级体系结构及其与其它云基础设施组件的关系的简化方框图；

[0049] 图26C是图解说明按照本发明的实施例的利用Nuviaq系统的服务开通处理的步骤的例证序列图；

[0050] 图26D是图解说明按照本发明的实施例的利用Nuviaq系统的部署处理的步骤的例证序列图；

[0051] 图26E是按照本发明的实施例，为数据库服务提供的数据库实例的例子；

[0052] 图27描述按照本发明的实施例的计算设备的功能方框图；

[0053] 图28描述按照本发明的又一个实施例的计算设备的功能方框图。

[0054] 图29描述按照本发明的另一个实施例的计算设备的功能方框图。

具体实施方式

[0055] 在下面的说明中，为了说明起见，陈述了具体的细节，以透彻理解本发明的实施例。不过，显然可在没有这些具体细节的情况下，实践本发明。

[0056] 本发明的一些实施例提供使云基础设施系统提供的服务的开通(provisioning)、管理和跟踪自动化的技术。

[0057] 在一些实施例中，云基础设施系统可包括按照自助式的基于预订的可弹性缩放、可靠并且高度可用的安全方式，交付给客户的一批应用、中间件和数据库服务提供。这种云基础设施系统的例子是本受让人提供的Oracle Public Cloud。

[0058] 云基础设施系统可提供许多能力，包括(但不限于)开通、管理和跟踪客户对云基础设施系统中的服务和资源的预订，向利用云基础设施系统中的服务的客户提供可预测的运营费用，提供云基础设施系统中的客户数据的鲁棒的身份域分离和保护，向客户提供云基础设施系统的设计的透明架构和控制，向客户提供有保证的数据保护和对数据隐私标准和规定的遵守，向客户提供在云基础设施系统中建立和部署服务的集成开发体验，和向客户提供云基础设施系统中的商业软件、中间件、数据库和基础设施服务之间的无缝集成。

[0059] 在一些实施例中，云基础设施系统提供的服务可包括经请求，云基础设施系统的用户可以得到的许多服务，比如在线数据存储和备份解决方案、基于Web的电子邮件服务、托管的办公套件和文档协作服务、数据库处理、受管技术支持服务等。云基础设施系统提供的服务可动态缩放，以满足其用户的需求。这里，把云基础设施系统提供的服务的具体例示称为服务实例。通常，通过诸如因特网之类的通信网络，用户可从云服务提供者的系统获得的任何服务被称为云服务。一般，在公共云环境中，构成云服务提供者的系统的服务器和系统不同于客户自己的服务器和系统。例如，云服务提供者的服务可托管应用，用户可经请求通过诸如因特网之类的通信网络定购和使用所述应用。

[0060] 计算机网络云基础设施中的服务包括对存储器、托管的数据库、托管的web服务器、软件应用或云厂家向用户提供的其它服务，或者本领域已知的其它方面的受保护的计算机网络访问。例如，服务可包括通过因特网，对云上的远程存储器的受密码保护的访问。再例如，服务可包括供连网的开发人员专用的基于web服务的托管关系数据库和脚本-语言中间件引擎。又例如，服务可包括对托管在云厂商的网站上的电子邮件软件应用的访问。

[0061] 图20A是按照本发明的一个实施例的云基础设施系统的逻辑视图。云基础设施系统2000可通过云或连网环境，提供各种服务。这些服务可包括按照软件即服务(SaaS)类别、平台即服务(PaaS)类别、基础设施即服务(IaaS)类别、或者其它服务类别(包括混合服务)提供的一种或多种服务。借助预订定单，客户可定购云基础设施系统2000提供的一种或多种服务。云基础设施系统2000随后进行处理，以提供客户的预订定单中的服务。

[0062] 云基础设施系统2000可通过不同的部署模型，提供云服务。例如，可按照其中云基础设施系统2000由出售云服务的机构拥有(例如，由Oracle拥有)、公众或不同的工业企业可以获得服务的公共云模型，来提供服务。再例如，可按照其中只为单一机构运营云基础设施系统2000、云基础设施系统2000可为该机构内的一个或多个实体提供服务的专用云模

型，来提供服务。也可按照其中云基础设施系统2000和系统2000提供的服务由相关社区中的几个机构共享的社区云模型，来提供云服务。也可按照混合云模型，来提供云服务，混合云模型是两种或更多种不同模型的组合。

[0063] 如图20A中所示，云基础设施系统2000包括多个组件，协同工作的所述多个组件能够实现云基础设施系统2000提供的服务的开通。在图20A中图解所示的实施例中，云基础设施系统2000包括SaaS平台2002、PaaS平台2004、IaaS平台2010、基础设施资源2006和云管理功能2008。这些组件可用硬件或软件，或者它们的组合来实现。

[0064] SaaS平台2002被配置成提供被归入SaaS类别的云服务。例如，SaaS平台2002可提供在集成的开发和部署平台上，建立和交付一套按需应用的能力。SaaS平台2002可管理和控制底层软件和基础设施，以提供SaaS服务。通过利用SaaS平台2002提供的服务，客户能够利用在云基础设施系统2000上运行的应用。客户能够获得应用服务，而不需要客户购买单独的许可证和支持。

[0065] 可以提供各种不同的SaaS服务。例子包括(但不限于)为销售业绩管理、大型机构的企业整合和商业灵活性等提供解决方案的服务。在一个实施例中，SaaS服务可包括Customer Relationship Management(CRM)服务2010(例如，利用Oracle云提供的Fusion CRM服务)，Human Capital Management(HCM)/Talent Management服务2012等。CRM服务2010可包括目的在于向客户报告及管理销售活动周期的服务，以及其它服务。HCM/Talent服务2012可包括目的在于向客户提供全球劳动力生命周期管理和人才管理服务的服务。

[0066] 各种不同的PaaS服务可由PaaS平台2004在标准化、共享和可弹性缩放的应用开发和部署平台中提供。PaaS服务的例子可包括(但不限于)使机构(比如Oracle)能够在共享的公共体系结构上整合现有的应用的服务，以及建立充分利用平台提供的共享服务的新应用的能力。PaaS平台2004可管理和控制底层软件和基础设施，以提供PaaS服务。客户可获得云基础设施系统2000提供的PaaS服务，而不需要客户购买单独的许可证和支持。PaaS服务的例子包括(但不限于)Oracle Java Cloud Service(JCS)、Oracle Database Cloud Service(DBCS)及其它。

[0067] 通过利用PaaS平台2004提供的服务，客户能够利用云基础设施系统2000支持的编程语言和工具，还能够控制部署的服务。在一些实施例中，云基础设施系统2000提供的PaaS服务可包括数据库云服务2014、中间件云服务(例如，Oracle Fusion Middleware服务)2016和Java云服务2017。在一个实施例中，数据库云服务2014可支持使机构能够汇聚数据库资源并以数据库云的形式向客户提供数据库即服务的共享服务部署模型，中间件云服务2016向客户提供开发和部署各种商业应用的平台，Java云服务2017向客户提供在云基础设施系统2000中部署Java应用的平台。图20A中图解所示的SaaS平台2002和PaaS平台2004中的组件只是用于举例说明，并不意图限制本发明的实施例的范围。在备选实施例中，SaaS平台2002和PaaS平台2004可包括向云基础设施系统2000的客户提供另外的服务的附加组件。

[0068] IaaS平台2010可提供各种不同的IaaS服务。IaaS服务便利底层计算资源，比如存储器、网络、和供客户利用SaaS平台和Paas平台提供的服务的其它基本计算资源的管理和控制。

[0069] 在一些实施例中，云基础设施系统2000包括提供用于向云基础设施系统2000的客户提供各种服务的资源的基础设施资源2006。在一个实施例中，基础设施资源2006包括诸

如服务器、存储器和连网资源之类硬件的预先集成和优化的组合，以执行PaaS平台和SaaS平台提供的服务。

[0070] 在一些实施例中，云管理功能2008提供云基础设施系统2000中的云服务(例如，SaaS、PaaS、IaaS服务)的全面管理。在一个实施例中，云管理功能2008包括开通、管理和跟踪云基础设施系统2000接收的客户的预订等的能力等。

[0071] 图20B是用于实现按照本发明的实施例的云基础设施系统2000的硬件/软件栈的简化方框图。应理解图20B中描述的实现可具有除图20B中所示的组件外的其它组件。此外，图20B中所示的实施例只是可包含本发明的实施例的云基础设施系统的一个例子。在一些其它实施例中，云基础设施系统2000可具有比图20B中所示的组件更多或更少的组件，可以组合两个或者更多的组件，或者可以具有组件的不同结构或排列。在一些实施例中，硬件和软件组件被堆叠，以便形成提供最佳性能的垂直集成。

[0072] 各种用户可与云基础设施系统2000交互作用。例如，这些用户可包括能够利用各种客户端设备，比如桌上型计算机、移动设备、平板计算机等，与云基础设施系统2000交互的最终用户2050。用户还可包括利用命令行接口(CLI)、应用编程接口(API)，通过各种集成开发环境(IDE)，以及借助其它应用，与云基础设施系统2000交互作用的开发人员/编程人员2052。用户还可包括运行人员2054。运行人员可包括云服务提供者的职员或者其他用户的职员。

[0073] 应用服务层2056识别可由云基础设施系统2000提供的各种云服务。通过服务集成和连接层2058，这些服务可被映射到或者与相应的软件组件2060(例如，提供Java服务的Oracle WebLogic服务器，提供数据库服务的oracle数据库，等等)关联。

[0074] 在一些实施例中，可以提供由云基础设施系统2000的不同组件或模块共享，以及由云基础设施系统2000提供的服务共享的许多内部服务2062。这些内部的共享服务可包括(但不限于)安全和身份服务，集成服务，企业储存库服务，企业管理员服务，病毒扫描和白名单服务，高可用性、备用和恢复服务，能够在IDE中实现云支持的服务，电子邮件服务，通知服务，文件传输服务，等等。

[0075] 运行时基础设施层2064表示在其上建立各种其它层和组件的硬件层。在一些实施例中，运行时基础设施层2064可包含用于提供存储、处理和连网资源的一个Oracle的Exadata机器。Exadata机器可由各种数据库服务器、存储服务器、连网资源、和用于托管与云服务相关的软件层的其它组件构成。在一些实施例中，Exadata机器可被设计成和Oracle Exalogic一起工作，Oracle Exalogic是提供存储、计算、网络和软件资源的集合的工程化系统。Exadata和Exalogic的组合提供交付用于提供云服务的高性能、高度可用、可缩放、安全并且可控制的平台的完全的硬件和软件工程化解决方案。

[0076] 图21是按照本发明的实施例，实现图20A中所示的云基础设施系统的系统环境的简化方框图。在图解所示的实施例中，系统环境2310包括可被用户用于与云基础设施系统2000交互作用的一个或多个客户端计算设备2124、2126和2128。客户端设备可被配置成运行可被客户端设备的用户用于与云基础设施系统2000交互作用，以利用云基础设施系统2000提供的服务的客户端应用，比如web浏览器、专用客户端应用(例如，Oracle Forms)或一些其它应用。

[0077] 应理解图21中所示的云基础设施系统2000可以具有除图21中所示的组件之外的

其它组件。此外，图21中所示的实施例只是可包含本发明的实施例的云基础设施系统的一个例子。在一些其它实施例中，云基础设施系统2000可具有比图21中所示的组件更多或更少的组件，可以组合两个或更多的组件，或者可以具有组件的不同结构或排列。

[0078] 客户端计算设备2124、2126和2128可以是通用个人计算机(例如，包括运行各种版本的Microsoft Windows和/或Apple Macintosh操作系统的个人计算机和/或膝上型计算机)、蜂窝电话机或PDA(运行诸如Microsoft Windows Mobile之类的软件，并且允许因特网、电子邮件、SMS、Blackberry或其它通信协议)、运行各种可从市场获得的UNIX或UNIX似的操作系统(包括(但不限于)各种GNU/Linux操作系统)任意之一的工作站计算机、或者任何其它计算设备。例如，客户端计算设备2124、2126和2128可以是能够通过网络(例如，下面说明的网络2132)通信的任何其它电子设备，比如精简型客户端计算机、允许因特网的游戏系统、和/或个人消息接发设备。尽管例证的系统环境2130被表示成具有3个客户端计算设备，不过可以支持任意数目的客户端计算设备。诸如带传感器的设备之类的其它设备可以与云基础设施系统2000交互作用。

[0079] 网络2132可便利客户端2124、2126和2128与云基础设施系统2000之间的通信和数据交换。网络2132可以是本领域的技术人员熟悉的可利用各种可从市场获得的协议，包括(但不限于)TCP/IP、SNA、PX、AppleTalk等任意之一而支持数据通信的任意种类的网络。仅仅作为例子，网络2132可以是诸如以太网、令牌环网络之类的局域网(LAN)，广域网，虚拟网络，包括(但不限于)虚拟专用网(VPN)，因特网，企业内部网，外联网，公共交换电话网(PSTN)，红外网络，无线网络(例如，按照IEEE 802.1X协议套件，本领域已知的蓝牙协议，和/或任何其它无线协议任意之一运行的网络)，和/或这些和/或其它网络的任何组合。

[0080] 云基础设施系统2000可包含一个或多个计算机和/或服务器，所述计算机和/或服务器可以是通用计算机、专用服务器计算机(例如，包括PC服务器、UNIX服务器、中程服务器、大型计算机、机架安装服务器等)、服务器群、服务器群集、或者任何其它适当的排列和/或组合。构成云基础设施系统2000的计算设备可以运行任意操作系统或者各种另外的服务器应用和/或中间层应用，包括HTTP服务器、FTP服务器、CGI服务器、Java服务器、数据库服务器等。例证的数据库服务器包括(但不限于)可在市场上从Oracle、Microsoft、Sybase、IBM等获得的那些数据库服务器。

[0081] 在各个实施例中，云基础设施系统2000适合于自动开通、管理和跟踪客户对云基础设施系统2000提供的服务的预订。在一个实施例中，如图21中所示，云基础设施系统2000中的组件包括身份管理(IDM)模块2100，服务模块2102，租户自动化系统(TAS)模块2104，服务部署基础设施(SDI)模块2106，企业管理器(EM)模块2108，一个或多个前端web接口，比如存储库用户接口(UI)2110、云用户接口(UI)2112和支持用户接口(UI)2116，定单管理模块2114，销售人员2118，运营商人员2120和定单数据库2142。这些模块可包括一个或多个计算机和/或服务器，或者可利用一个或多个计算机和/或服务器提供，所述计算机和/或服务器可以是通用计算机，专用服务器计算机，服务器群，服务器群集或者任何其它适当的排列和/或组合。在一个实施例中，这些模块中的一个或多个模块可由云基础设施系统2000中的云管理功能2008或IaaS平台2010提供。图21中所示的云基础设施系统2000中的各个模块只是用于举例说明，并不意图限制本发明的实施例的范围。备选实施例可以包括比图21中所示的组件更多或更少的模块。

[0082] 在例证操作中，在(1)，利用诸如客户端设备2124或2126之类客户端设备的客户通过浏览云基础设施系统2000提供的各种服务，并发出预订云基础设施系统2000提供的一种或多种服务的定单，可与云基础设施系统2000交互作用。在一些实施例中，客户可访问存储库UI 2110或云UI 2112，并通过这些用户接口发出预订定单。

[0083] 响应客户发出定单，云基础设施系统2000接收的定单信息可包括识别客户和客户打算预订的云基础设施系统2000提供的一种或多种服务的信息。单个定单可包括对多个服务的定购。例如，客户可登录到云UI 2112，在相同的定单中请求对CRM服务和Java云服务的预订。

[0084] 另外，定单还可包括定购的服务的一个或多个服务水平。如这里所用和下面更详细讨论的那样，服务的服务水平确定为在预订的上下文中提供请求的服务而分配的资源的数量，比如存储器的数量，计算资源的数量，数据传输设施等。例如，基本服务水平可提供最低程度的存储器、数据传输、或者用户数量，而更高的服务水平可包括额外的资源。

[0085] 另外，在一些情况下，云基础设施系统2000接收的定单信息中包括表示客户级别，和期望所述服务的时段的信息。客户级别规定客户进行预订请求的优先级。在一个例子中，可根据如在客户和云服务的提供者之间达成的Service Level Agreement(SLA)规定的云基础设施系统2000向客户保证或承诺的服务质量，来确定优先级。在一个例子中，不同的客户级别包括基本级，白银级和黄金级。服务的时段可指定服务的开始日期和时间，以及期望所述服务的时段(例如，可以指定服务结束日期和时间)。

[0086] 在一个实施例中，客户可通过存储库UI 2110请求新的预订，或者通过云UI 2112请求试预订。在一些实施例中，存储库UI 2110可代表服务提供者的电子商务存储库前端(例如，Oracle云服务的www.oracle.com/store)。云UI 2112可代表服务提供者的商业接口。客户可通过云UI 2112考察可用的服务，和签约感兴趣的服务。云UI 2112捕捉为定购云基础设施系统2000提供的试预订所必需的用户输入。云UI 2112还可用于查看账户特征，和配置位于云基础设施系统2000内的运行时环境。除了发出对新预订的定单之外，存储库UI 2110还使客户能够进行其它与预订相关的任务，比如改变预订的服务水平，延长预订的期限，提高预订的服务水平，终止现有的预订，等等。

[0087] 在按(1)发出定单之后，在(2)，通过存储库UI 2110或云2112收到的定单信息被保存在定单数据库2142中，定单数据库2142可以是云基础设施系统2000操作、并且结合其它系统元件使用的几个数据库之一。尽管在图21中，定单数据库2142逻辑上被表示成单一数据库，不过在实际的实现中，定单数据库可包含一个或多个数据库。

[0088] 在(3)，定单被转发给定单管理模块2114。定单管理模块2114被配置成进行与定单相关的记账和结算功能，比如核实定单，并依据所述核实，登记定单。在一些实施例中，定单管理模块2114可包括合同管理模块和安装基础模块。合同管理模块可保存与客户的预订定单相关的合同信息，比如客户与云基础设施系统2000的服务水平协议(SLA)。安装基础模块可包括客户的预订定单中的服务的详细说明。除了定单信息之外，安装基础模块可跟踪与服务相关的安装细节，产品状态和与服务相关的支持服务历史。当客户定购新的服务或者升级现有服务时，安装基础模块可自动增加新的定单信息。

[0089] 在(4)，和定单有关的信息被传送给TAS模块2104。在一个实施例中，TAS模块2104利用定单信息编排用于客户发出的定单的服务和资源的调配。在(5)，TAS组件2104编排资

源的调配，以利用SDI模块2106的服务，支持预订的服务。在(6)，TAS模块2104把与从SDI模块2106接收的开通服务的定单有关的信息提供给服务模块2102。在一些实施例中，在(7)，SDI模块2106还可利用服务模块2102提供的服务来分配和配置为满足客户的预订定单而需要的资源。

[0090] 在(8)，服务模块2102把关于定单的状态的通知发送给在客户端设备2124、2126和2128上的客户。

[0091] 在一些实施例中，TAS模块2104起管理与各个定单相关的商业过程，和应用商业逻辑以确定定单是否应着手进行服务开通的编排组件的作用。在一个实施例中，当收到对新预订的定单时，TAS模块2104向SDI模块2106发送请求，以分配为满足该预订定单所需的资源和配置这些资源。SDI模块2106使得能够为客户定购的服务分配资源。SDI模块2106提供云基础设施系统2000提供的云服务和用于开通提供所请求的服务的资源的物理实现层之间的抽象层次。TAS模块2104从而可以与诸如服务和资源是否实际上是即时调配的，还是预先调配的，只不过应请求被分配/分派之类实现细节隔离。

[0092] 在一些实施例中，用户可利用存储库UI 2110直接与定单管理模块2114交互作用，进行与记账和结算相关的功能，比如核实定单，并依据所述核实，登记定单。在一些实施例中，代替客户发出定单，在(9)，定单可改为由代表客户的销售人员2118(比如客户的服务代表或者销售代表)发出。销售人员2118可通过定单管理模块2114提供的用户接口(图21中未图示)，直接与定单管理模块2114交互作用，以便发出定单或者向客户提供报价。例如，对于大客户可以实现这种特征，其中定单可由客户的销售代表通过定单管理模块2114发出。销售代表可代表客户提出预约。

[0093] EM模块2108被配置成监控与在云基础设施系统2000中，管理和跟踪客户的预订相关的活动。EM模块2108收集预订定单中的服务的使用统计信息，比如使用的存储量，传送的数据量，用户的数目，系统工作时间和停机时间的数量。在(10)，主运营商人员2120(可以是云基础设施系统2000的提供者的雇员)可以通过企业管理器用户接口(图21中未图示)，与EM模块2108交互作用，以管理云基础设施系统2000内，基于其开通服务的系统和资源。

[0094] 身份管理(IDM)模块2100被配置成提供云基础设施系统2000中的身份服务，比如访问管理和授权服务。在一个实施例中，IDM模块2100控制和希望利用云基础设施系统2000提供的服务的客户有关的信息。这种信息可包括验证所述客户的身份的信息，和说明这些客户被准许对各种系统资源(例如，文件、目录、应用、通信端口、存储段等)，进行哪些操作的信息。IDM模块2100还可包括关于各个客户的描述信息，以及所述描述信息可被谁如何访问和变更的管理。

[0095] 在一个实施例中，身份管理模块2100管理的信息可被分区，以创建单独的身份域。属于特定身份域的信息可以与所有其它身份域隔开。另外，身份域可被多个单独的租户共享。每个所述租户可以是预订云基础设施系统2000中的服务的客户。在一些实施例中，客户可以具有一个或多个身份域，每个身份域可以与一个或多个预订相关，每个预订具有一个或多个服务。例如，单一客户可代表大型实体，可为所述大型实体内的分部/部门创建身份域。EM模块2108和IDM模块2100可分别依次在(11)和(12)与定单管理模块2114交互作用，以在云基础设施系统2000中管理和跟踪客户的预订。

[0096] 在一个实施例中，在(13)，通过支持UI 2116，也可向客户提供支持服务。在一个实

施例中，支持UI 2116使支持人员能够通过支持后端系统，与定单管理模块2114交互作用，以在(14)进行支持服务。云基础设施系统2000中的支持人员以及客户可以通过支持UI 2116，提交程序缺陷报告，和检查这些报告的状态。

[0097] 云基础设施系统2000还可提供图21中未图示的其它接口。例如，身份域管理员可利用与IDM模块2100的用户接口来配置域和用户身份。另外，客户可登录他们希望利用的每种服务的单独接口。在一些实施例中，希望预订云基础设施系统2000提供的一种或多种服务的客户还可被分派各种角色和职责。在一个实施例中，对于客户可分派的不同角色和职责可包括购买者、账户管理员、服务管理员、身份域管理员或者利用云基础设施系统2000提供的服务和资源的用户的角色和职责。下面在图23中，更充分地说明不同的角色和职责。

[0098] 图22A是按照本发明的实施例，说明由云基础设施系统中的TAS模块进行的处理的简化流程图2200。图22A中所示的处理可用由一个或多个处理器执行的软件(例如，代码、指令、程序)、硬件或者软件和硬件的组合来实现。软件可被保存在存储器(例如，存储设备，非临时性计算机可读存储介质)上。图22A中所示的特定的一系列处理步骤并不是限制性的。按照备选实施例，也可进行其它步骤序列。例如，本发明的备选实施例可以按照不同的顺序，进行上面概述的步骤。此外，图22A中图解所示的各个步骤可包括可按照适合于各个步骤的各种顺序进行的多个子步骤。此外，取决于特定应用，可以增加或删除另外的步骤。本领域的技术人员会认识到许多变化、修改和替换。在一些实施例中，图22A中所示的处理可由TAS组件2104中的一个或多个组件进行，如在图22B中详细所述。

[0099] 在2202，处理客户的预订定单。在一个例子中，处理可包括确认定单。确认定单包括确保客户已支付预订的费用，和确保客户不具有名称相同的预订，或者对于不允许客户在相同身份域中创建相同类型的多个预订的预订类型(例如，在CRM服务的情况下)，确保客户未企图在相同身份域中创建相同类型的多个预订。处理还可包括对于云基础设施系统2000正在处理的各个定单，跟踪定单的状态。

[0100] 在2204，识别与定单相关的商业过程。在一些情况下，对于定单，可以识别多个商业过程。每个商业过程识别处理定单的各个方面的一系列步骤。例如，第一商业过程可识别与为定单调配物理资源相关的一个或多个步骤，第二商业过程可识别与创建身份域以及定单的客户身份有关的一个或多个步骤，第三商业过程可识别与进行后台功能，比如为用户创建客户记录，进行与定单相关的结算功能等有关的一个或多个步骤。在一些实施例中，还可识别不同的商业过程，以处理定单中的不同服务。例如，可以识别不同的商业过程，以处理CRM服务和数据库服务。

[0101] 在2206，执行在2204对于定单识别的商业过程。执行与定单相关的商业过程可包括编排与在步骤2204中识别的商业过程相关的一系列步骤。例如，执行与为定单调配物理资源相关的商业过程可包括向SDI模块2106发送请求，以分配为满足预订定单所需的资源和配置这些资源。

[0102] 在2208，把关于调配的定单的状态的通知发送给客户。在图22B中详细提供了与进行步骤2202、2204、2206和2208相关的其它说明。

[0103] 图22B是按照本发明的实施例，说明云基础设施系统中的TAS模块中的一个或多个子模块的简化高级示图。在一个实施例中，在图22B中所示的模块进行在图22A中讨论的步骤2202-308中说明的处理。在图解所示的实施例中，TAS模块2104包括定单处理模块2210、

商业过程识别器2212、商业过程执行器2216、超额(overage)架构2222、工作流标识模块2224和捆绑预订生成器模块2226。这些模块可用硬件或软件，或者硬件和软件的组合来实现。图22B中所示的TAS模块的各个模块只是用于举例说明，并不意图限制本发明的实施例的范围。备选实施例可以包括比图22B中所示的模块更多或更少的模块。

[0104] 在一个实施例中，定单处理模块2210从一个或多个输入源2221，接收来自客户的定单。例如，在一个实施例中，定单处理模块2210可通过云UI 2112或存储库UI 2110，直接接收定单。另一方面，定单处理模块2210可从定单管理模块2114或定单数据库2142，接收定单。定单处理模块2210随后处理定单。在一些实施例中，处理定单包括生成客户记录，客户记录包括与定单有关的信息，比如服务类型、服务水平、客户级别、资源的种类、待分配给服务实例的资源的数量、和期望所述服务的时段。作为所述处理的一部分，定单处理模块2210还判定定单是否是有效定单。这包括确保客户不已经具有名称相同的预订，或者对于不允许客户在相同身份域中创建相同类型的多个预订的预订类型(例如，在融合CRM服务的情况下)，确保客户未企图在相同身份域中创建相同类型的多个预订。

[0105] 定单处理模块2210还可对定单进行另外的处理。处理可包括对于云基础设施系统2000处理的各个定单，跟踪定单的状态。在一个实施例中，定单处理模块2210可处理各个定单，以识别和该定单有关的许多状态。在一个例子中，定单的不同状态可以是初始化状态，调配状态，有效状态，需要管理状态，出错状态等。初始化状态指的是新定单的状态；调配状态指的是一旦用于定单的服务和资源被调配时的定单的状态。当定单已被TAS模块2104处理，并且关于此的通知被传送给客户时，定单处于有效状态。当需要管理员的干预，以解决问题时，定单处于需要管理状态。当定单不能被处理时，定单处于出错状态。除了保持定单进展状态之外，定单处理模块2210还保持和在处理执行期间遇到的任何故障有关的详细信息。在其它实施例中，并且如下详细所述，定单处理模块2210进行的另外的处理还包括改变预订中的服务的服务水平，改变包含在预订中的服务，延长预订的时段，和取消预订或者指定预订中的不同时段的不同服务水平。

[0106] 在定单处理模块2210处理了定单之后，应用商业逻辑，以确定是否应着手调配该定单。在一个实施例中，作为编排定单的一部分，商业过程识别器2212从定单处理模块2210接收处理后的定单，并应用商业逻辑，以识别用于正在处理的定单的特定商业过程。在一个实施例中，商业过程识别器2212可利用保存在服务目录2214中的信息来确定用于定单的商业过程。在一个实施例中，并且如在图22中所述，对于一个定单可以识别多个商业过程，每个商业过程识别用于处理定单的各个方面的一系列步骤。在另一个实施例中，并且如上所述，对于不同类型的服务，或者诸如CRM服务或数据库服务之类的服务的组合，可以定义不同的商业过程。在一个实施例中，服务目录2214可保存把定单映射到特定类型的商业过程的信息。商业过程识别器2212可利用该信息来识别用于正被处理的定单的特定商业过程。

[0107] 一旦识别了商业过程，商业过程识别器2212就把待执行的特定商业过程传送给商业过程执行器2216。商业过程执行器2216随后通过与云基础设施系统2000中的一个或多个模块协同工作，执行识别的商业过程的步骤。在一些实施例中，商业过程执行器2216起进行与商业过程相关的步骤的编排器的作用。例如，商业过程执行器可以与定单处理模块2210交互作用，以执行识别与定单相关的工作流、确定定单中的服务的超额(overage)或者识别与定单相关的服务组件的商业过程中的步骤。

[0108] 在一个例子中，商业过程执行器2216与SDI模块2106交互作用，以执行为在预订定单中请求的服务分配和调配资源的商业过程中的步骤。在这个例子中，对于商业过程中的各个步骤，商业过程执行器2216可向SDI组件2106发送请求，以分配和配置为满足特定步骤而需要的资源。SDI组件2106负责资源的实际分配。一旦执行了定单的商业过程的所有步骤，商业过程执行器2216可通过利用服务组件2102的服务，向已处理定单的客户发送通知。所述通知可包括向客户发送带有已处理定单的详情的电子邮件通知。电子邮件通知还可包括与定单相关的部署信息，以使客户能够访问预订的服务。

[0109] 在一些实施例中，TAS模块2104可提供使TAS模块2104能够与云基础设施系统2000中的其它模块交互作用，和对于其它模块，与TAS模块2104交互作用的一个或多个TAS应用编程接口(API)2218。例如，TAS API可包括通过基于异步Simple Object Access Protocol(SOAP)web服务调用与SDI模块2106交互作用，以便为客户的预订定单调配资源的系统服务开通API。在一个实施例中，TAS模块2104还可利用系统服务开通API来完成系统和服务实例创建和删除，把服务实例切换到提高的服务水平，和关联服务实例。这种情况的一个例子是Java服务实例与融合应用服务实例的关联，以允许安全的web服务通信。TAS API还可包括与服务模块2102交互作用，以把已处理定单通知客户的通知API。在一些实施例中，TAS模块2104还定期把预订信息，停歇期和通知(例如，计划的停机时间)传送给服务组件2102。

[0110] 在一些实施例中，TAS模块2104定期从EM模块2108，接收关于各个开通的服务的使用统计信息，比如使用的存储量，传送的数据量，用户的数目，和系统工作时间和停机时间的数量。超额(overage)架构2222利用使用统计信息来判定是否出现服务的使用过度，如果是，那么判定对于所述超额要计费多少，并把该信息提供给定单管理模块2114。

[0111] 在一些实施例中，TAS模块2104包括配置成识别与处理客户的预订定单相关的一个或多个工作流的定单工作流识别模块2224。在一些实施例中，TAS模块2104可包括当客户发出对于云基础设施系统2000提供的一种或多种服务的预订定单时，为客户生成预订定单的预订定单生成架构2226。在一个实施例中，预订定单包括负责提供预订定单中的客户请求的服务的一个或多个服务组件。

[0112] 另外，TAS模块2104还可与一个或多个另外的数据库(比如Tenant Information System(TIS)数据库2220)交互作用，以使得能够在考虑可供客户利用的历史信息(如果有的话)的时候，实现用于客户预订的一个或多个服务的资源的调配。TIS数据库2220可包括与客户预订的定单有关的历史定单信息和历史使用信息。

[0113] 可利用不同的部署模型，部署TAS模块2104。在一些实施例中，所述部署包括与一个或多个分布式组件进行接口的中心组件。例如，分布式组件可被部署成各个数据中心，从而也可被称为数据中心组件。中心组件包括处理定单和协调云基础设施系统2000中的服务的能力，而数据中心组件提供开通和运行为预订服务提供资源的运行时系统的能力。

[0114] 图23按照本发明的实施例，说明TAS模块的例证分布式部署。在图23中所示的实施例中，TAS模块2104的分布式部署包括TAS中心组件2300和一个或多个TAS数据中心(DC)组件2302、2304和2306。这些组件可以用硬件或软件，或者硬件和软件的组合来实现。

[0115] 在一个实施例中，TAS中心组件2300的职责包括(但不限于)提供中央组件，用于接收客户定单，进行与定单相关的商业操作，比如创建新预订，变更预订中的服务的服务水平，变更包含在预订中的服务，和延长预订的时段，或者取消预订。TAS中心组件2300的职责

还包括保持和供给云基础设施系统2000所需的预订数据，和与定单管理模块2114、支持UI 2116、云UI 2112和存储库UI 2110接口，以处理所有的后台交互作用。

[0116] 在一个实施例中，TAS CS 2302、2304和2306的职责包括(但不限于)进行运行时操作，以便编排用于客户预订的一个或多个服务的资源的调配。TAS DC 2302、2304和2306还包括进行诸如锁定、解锁、允许或禁止预订定单，收集与定单相关的指标，确定定单的状态，和发送与定单相关的通知事件之类的操作。

[0117] 在图23中所示的分布式TAS系统的例证操作中，TAS中心组件2300最初通过云UI 2112、存储库UI 2110，通过定单管理模块2114，或者通过定单数据库2142，接收来自客户的定单。在一个实施例中，客户代表具有金融信息和定购和/或变更预订的权限的购买者。在一个实施例中，定单信息包括识别客户，客户希望预订的服务的类型，和负责处理请求的账户管理员的信息。在一些实施例中，当客户发出预订云基础设施系统2000提供的一种或多种服务的定单时，账户管理员可由客户指派。根据定单信息，TAS中心组件2300识别定单起源于的世界的数据地区，比如美洲、EMEA或亚太，和为了调配所述定单而要部署的特定TAS DC(例如，2302、2304或2306)。在一个实施例中，为了调配所述定单而要部署的特定TAS DC(例如，出自DC 2302、2304或2306中)是根据请求起源于的地理数据地区确定的。

[0118] TAS中心组件2300随后把定单请求发送给其中将开通定单请求的服务的特定TAS DC。在一个实施例中，TAS DC 2302、2304或2306识别在该特定TAS DC，负责处理定单请求的服务管理员和身份域管理员。服务管理员和身份域管理员可由在预订定单中识别的账户管理员指派。TAS DC 2302、2304或2306与SDI模块2104通信，以编排供定单之用的物理资源的调配。各个TAS DC 2302、2304或2306中的SDI组件2104分配并配置为满足预订定单所需要的那些资源。

[0119] 在一些实施例中，TAS DC 2302、2304或2306识别与预订相关的身份域。SDI组件2106可把身份域信息提供给IDM组件2100(示于图21中)，以识别现有的身份域或创建新的身份域。一旦定单被在相应TAS DC 2302、2304或2306的SDI模块调配，TAS中心组件2300就可通过支持UI 2116，发出与支持系统中的调配的资源有关的信息。例如，信息可包括显示与服务相关的资源指标，和服务的使用统计信息。

[0120] 一旦在运转中，在各个数据中心，EM模块2108定期收集在该数据中心开通的各个已开通服务的使用统计信息，比如使用的存储量，传送的数据量，用户的数目，和系统工作时间及停机时间的数量。这些统计信息被提供给在EM模块2108本地(即，在相同的数据中心)的TAS DC。在实施例中，TAS DC可以利用使用统计信息来确定是否发生了服务的使用过度，如果是，那么确定对于所述超额要计费多少，并把计费信息提供给定单管理模块2114。

[0121] 图24是按照本发明的实施例，图解说明SDI模块与云基础设施系统中的一个或多个模块的交互作用的简化方框图。在一个实施例中，SDI模块2106与TAS模块2104交互作用，以便为在TAS模块2104接收的预订定单中的服务调配资源。在一些实施例中，图24中图解所示的一个或多个模块可以是云基础设施系统2000内的模块。在其它实施例中，与SDI模块2106交互作用的一个或多个模块可以在云基础设施系统2000外。另外，备选实施例可以具有比图24中所示的模块更多或更少的模块。这些模块可以用硬件、软件或者硬件和软件的组合来实现。

[0122] 在一个实施例中，SDI模块2106中的模块可包括云基础设施系统2000中的SaaS平

台2002和PaaS平台2004中的一个或多个模块。为了进行用于各种服务的资源的调配，SDI模块2106可与各个其它模块交互作用，所述各个其它模块都被定制成帮助用于特定类型的服务的资源的调配。例如，如在图24中图解所示，SDI模块2106可以与Java服务开通控制模块2400交互作用，以开通Java云服务。在一个实施例中，Java服务开通控制模块2400可部署由SDI模块2106指定的Java Cloud Service(JCS)集合，所述集合包括为了开通Java云服务而要进行的一组任务。基础设施资源2006随后确定为开通Java云服务而需要的资源。

[0123] 作为其它例子，SDI模块2106可以与一个或多个模块，比如Virtual Assembly Builder(VAB)模块2402，Application Express(APEX)部署器模块2404，Virtual Machine(VM)模块2406，IDM模块2100和数据库机器模块2018交互作用。VAB模块2402包括配置和提供完整的多层应用环境的能力。在一个实施例中，VAB模块2402利用VM模块2406提供的服务，部署SDI模块2106指定的Middleware(MW)服务集合，以在云基础设施系统2000中开通MW服务。APEX部署器模块2404包括配置和开通数据库服务的能力。在一个实施例中，APEX部署器模块2404利用基础设施资源2006提供的资源，部署SID模块2106指定的数据库服务集合，以在云基础设施系统2000中开通数据库服务。SDI模块2106与IDM模块2100交互作用，以提供诸如跨云基础设施系统2000中的多个应用的访问管理之类的身份服务。

[0124] 图25描述按照本发明的实施例的SDI模块的子模块的简化高级示图。在图25中所示的实施例中，SDI模块2106包括SDI-Web Services(WS)模块2500，SDI请求控制器模块2502，SDI任务管理器模块2504，SDI监控模块2506，SDI数据存取模块2508，SDI公用库模块2510和SDI连接器模块2512。这些模块可用硬件或软件，或者它们的组合实现。图25中所示的SDI模块2106及其各个模块只是用于举例说明，并不意图限制本发明的实施例的范围。备选实施例可以具有比图25中所示更多或更少的模块。下面详细说明这些模块及其功能。

[0125] SDI-WS模块2500包括从TAS组件2104的商业过程执行器2216，接收与定单相关的商业过程中的步骤的能力。在一个实施例中，SDI-WS模块2500解析商业过程的各个步骤，把该步骤转换成SDI模块2106使用的内部表示。在一个实施例中，与定单相关的商业过程的各个步骤以对SDI-WS模块2500的SOAP请求的形式，通过web服务处理层(例如，通过图22B中讨论的System Provisioning API)到达。

[0126] SDI请求控制器模块2502是SDI模块2106中的内部请求处理引擎，包括进行与定单请求相关的异步请求处理，并发请求处理，并发任务处理，容错和恢复，和插件支持。在一个实施例中，SDI请求控制器模块2502从SDI-WS模块2500，接受与定单相关的商业过程的各个步骤，并把该步骤提交给SDI任务管理器模块2504。

[0127] SDI任务管理器模块2504把在商业过程中指定的各个步骤转换成用于调配该特定步骤的一系列任务。一旦特定步骤的一组任务已被调配，SDI任务管理器模块2504就用包括具有为实现该特定步骤而调配的资源的细节的定单有效负载的操作结果，来响应TAS模块2104中的商业过程执行器2216。SDI任务管理器模块2504重复该过程，直到与定单相关的特定商业过程的所有步骤都完成为止。

[0128] 在一些实施例中，SDI任务管理器模块2504通过利用SDI连接器模块2512的服务，把在商业过程中指定的各个步骤转换成一系列的任务。SDI连接器模块2512包括用于由SDI任务管理器模块2504指定的任务的部署，以开通与定单请求相关的一个或多个服务的一个或多个连接器。在一些实施例中，连接器中的一个或多个连接器可处理特定于特定服务类

型的任务，而其它连接器可处理跨不同服务类型公共的任务。在一个实施例中，SDI连接器模块2512包括一组连接器(包装器API)，其与云基础设施系统2000中的外部模块(示于图24中)中的一个或多个外部模块进行接口，以开通与定单请求相关的服务和资源。例如，Application Express(APEX)连接器2514与APEX部署器模块2404进行接口，以开通数据库服务。Web Center Connector 2516(WCC)与云基础设施系统2000中的web中心模块面接，以开通web服务。web中心模块是用户参与平台，包括提供人和云基础设施系统2000中的信息之间的连接性的能力。

[0129] 在一些实施例中，Middleware Applications(MA)连接器2518与云基础设施系统2000中的VAB模块2402进行接口，以开通中间件应用服务。NUVIAQ连接器2520与VAB模块240进行接口，以开通Java服务。IDM连接器2522与IDM模块2100进行接口，以便为预订云基础设施系统2000中的服务和资源的用户提供身份和访问管理。Virtual Assembly Builder(VAB)连接器2524与云基础设施系统2000中的VAB模块2402进行接口，以配置和开通完整的多层应用环境。Plug-in连接器2526与EM模块2108进行接口，以管理和监控云基础设施系统2000中的组件。HTTP服务器连接器2528与PaaS平台中的一个或多个web服务器进行接口，以向云基础设施系统2000中的用户提供连接服务。

[0130] SDI模块2106中的SDI监控模块2506提供用于接收Java Management Extensions(JMX)请求的入站接口。SDI监控模块2506还提供用于管理和监控云基础设施系统2000中的应用、系统对象和设备的工具。SDI-数据存取模块2508提供用于接收Java Database Connectivity(JDBC)请求的入站接口。SDI-数据存取模块2508支持数据存取，提供云基础设施系统2000中的对象关系映射，java事务API服务，数据存取对象和连接池。SDI-公共库模块2510为SDI模块2106中的各个模块提供配置支持。

[0131] 上面讨论的图25的实施例说明按照本发明的实施例的SDI模块中的各个模块。图26A是按照本发明的实施例，说明由云基础设施系统中的SDI模块的各个模块进行的处理的简化流程图2600。图26A中描述的处理可用由一个或多个处理器执行的软件(例如，代码、指令、程序)、硬件或者软件和硬件的组合来实现。软件可被保存在存储器(例如，存储设备，非临时性计算机可读存储介质)上。图26A中所示的特定的一系列处理步骤并不是限制性的。按照备选实施例，也可进行其它步骤序列。例如，本发明的备选实施例可以按照不同的顺序，进行上面概述的步骤。此外，图26A中图解所示的各个步骤可包括可按照适合于各个步骤的各种顺序进行的多个子步骤。此外，取决于特定应用，可以增加或删除另外的步骤。本领域的技术人员会认识到许多变化、修改和替换。在一个实施例中，图26A中所示的处理可由在图25中详细说明的SDI模块2106中的一个或多个模块进行。

[0132] 在2602，接收与预订定单相关的商业过程。在一个实施例中，SDI模块2106中的SDI-WS模块2500从商业过程执行器2216，接收与预订定单相关的商业过程中的一个或多个步骤。在2604，商业过程中的各个步骤被转换成用于为预订定单调配资源的一系列任务。在一个实施例中，SDI模块2106中的SDI任务管理器模块2504通过利用SDI连接器模块2512的服务，把在商业过程中指定的各个步骤转换成一系列的任务。在2606，根据所述一系列任务，调配预订定单。在一个实施例中，并且如在图25中所示，SDI连接器模块2512包括用于处理由SDI任务管理器模块2504指定的任务的部署，以便为预订定单中的服务调配资源的一个或多个连接器。

[0133] 如上参考图25所述，SDI任务管理器模块2504通过利用SDI连接器模块2512的服务，把在商业过程中指定的各个步骤转换成一系列的任务，SDI连接器模块2512可包括用于处理由SDI任务管理器模块2504指定的任务的部署，以开通与定单请求相关的一个或多个服务的一个或多个连接器。连接器中的一个或多个连接器可处理特定于特定服务类型的任务，而其它连接器可处理跨不同服务类型公共的任务。在一个实施例中，SDI连接器模块2512包括与云基础设施系统2000中的外部模块(示于图24中)之中的一个或多个外部模块进行接口，以开通与定单请求相关的服务和资源的一组连接器(包装器API)。例如，NUVIAQ连接器2520与VAB模块2402进行接口，以开通Java服务。

[0134] 图26B是按照本发明的实施例，表示Nuviaq系统2610的高级体系结构及其与其它云基础设施组件的关系的简化方框图。应理解图26B中所示的Nuviaq系统2610可具有除图26B中所示的那些组件外的组件。此外，图26B中所示的实施例仅仅是可以具体体现本发明的实施例的云基础设施系统的例子。在一些其它实施例中，Nuviaq系统2610可具有比图26B中所示的组件更多或更少的组件，可以组合两个或更多的组件，或者可以具有组件的不同结构或排列。

[0135] 在一些实施例中，Nuviaq系统2610可被配置成提供用于编排PaaS操作的运行时引擎。Nuviaq系统2610可提供web服务API，以便利与其它产品和服务的集成。Nuviaq系统2610还提供对系统调配、应用部署和相关的生命周期操作中的复杂工作流的支持，并与管理和监控解决方案结合。

[0136] 在图26B中所示的实施例中，Nuviaq系统2610包括Nuviaq代理2612、Nuviaq管理器2614和Nuviaq数据库2616。在一些实施例中，Nuviaq管理器2614提供进入Nuviaq系统2610的入口点，从而提供经web服务API对PaaS操作的安全访问。在内部，它跟踪数据库中的系统状态，并控制在工作流引擎上的作业执行。在公共云中，Nuviaq管理器2614可被Tenant Provisioning系统(SDI 2106)和Tenant Console访问，以分别驱动调配和部署操作。

[0137] 在一个实施例中，Nuviaq管理器2614通过内部工作流引擎，异步执行作业。作业可以是特定于给定PaaS工作流的动作序列。可顺序进行动作，任何步骤中的故障导致整个作业的失败。许多工作流动作委托给与工作流相关的外部系统，比如EM命令行接口(cli)。在一种实现中，Nuviaq管理器2614应用可被托管在21-node WebLogic群集中，相关的HTTP服务器(例如，Oracle HTTP服务器或者说OHS)实例在防火墙内运行。

[0138] 在一些实施例中，Nuviaq代理2612是到Nuviaq API的公共接入点。在一个实施例中，这里只有公共API被暴露。代理2612接收的请求可被转发给Nuviaq管理器2614。在一个实施例中，Nuviaq代理2612在防火墙外运行，而管理器2614在防火墙内运行。在一种实现中，Nuviaq代理2612应用运行于在防火墙之外运行的WebLogic群集上。

[0139] 在一些实施例中，Nuviaq数据库2616跟踪各种域实体，比如(但不限于)平台实例、部署计划、应用、WebLogic域、作业、报警等。在适当的情况下，可使主键与服务数据库对准(align)。

[0140] 在一个实施例中，平台实例2618可包含为对于给定租户的WebLogic服务所需的所有资源。

[0141] Nuviaq系统2610可依靠云基础设施系统2000的其它系统来进行复用WebLogic云服务的工作流。这些依靠可包括对SDI 2106、IDM 2100、病毒扫描系统、服务数据库、CRM实

例等的依靠。例如,Nuviaq系统2610依靠由SDI 2106中的Assembly Deployer实现的功能。在一个实施例中,Assembly Deployer是管理与OVAB(Oracle Virtual Assembly Builder)和OVM(Oracle Virtual Machine)的交互作用的系统。Nuviaq系统2610使用的Assembly Deployer的能力可包括(但不限于)部署集合、解除部署集合、描述集合部署、缩放设备等的功能。在一种实现中,Nuviaq系统2610通过web服务API,访问Assembly Deployer。

[0142] 在一些实施例中,安全策略要求在某些工件(artifact)被部署到应用之前,对所述工件进行病毒扫描。云基础设施系统2000可提供用于此用途的病毒扫描系统,所述病毒扫描系统可以服务的形式,为公共云的多个组件提供扫描。

[0143] 在一些实施例中,公共云基础设施可保持包含关于租户(例如,客户)及其服务预订的信息的服务数据库。Nuviaq工作流可访问该数据,以便正确地把WebLogic服务配置成该租户也预订的其它服务的客户端。

[0144] 就其安全集成来说,云基础设施系统2000依靠IDM 2100。在一些实施例中,Java服务实例可以与CRM实例关联。这种关联允许部署到其Java服务实例的用户应用通过Web Service调用,访问CRM实例。

[0145] 各种实体可利用Nuviaq系统2610提供的服务。Nuviaq系统2610的这些客户端可包括:Tenant Console,它是客户可以访问,以管理他们的在其平台实例上的应用的基于管理服务器(例如,Oracle Management Server)的用户接口;已扩展到提供对应用生命周期管理操作的访问的几个IDE,比如Oracle IDE(JDeveloper、NetBeans和OEPE);可用于访问平台实例上的生命周期操作的一个或多个Command Line Interfaces(CLI)。

[0146] Nuviaq系统2610的服务开通使用情况-通过Nuviaq API的创建平台实例操作,实现服务开通平台实例使用情况。在云基础设施系统2000的上下文中,关于Nuviaq系统的服务实例对应于Nuviaq平台实例。平台实例被赋予在与该实例相关的所有后续操作时使用的唯一标识符。提供给创建平台实例动作的平台部署描述符允许设定变更平台实例的配置,以满足租户的预订要求的性质。例如,这些性质可包括:

[0147] Property#1:oracle.cloud.service.weblogic.size

[0148] 值:BASIC,STANDARD,ENTERPRISE

[0149] 说明:指定预订类型。这影响服务器的数目、数据库极限和服务设定的质量。

[0150] Property#2:oracle.cloud.service.weblogic.trial

[0151] 值:TRUE,FALSE

[0152] 说明:指示这是否是试预订。

[0153] Property#3:oracle.cloud.service.weblogic.crm

[0154] 值:CRM Service ID

[0155] 说明:识别将与该WebLogic服务实例相关的CRM服务。

[0156] 图26C是图解说明按照本发明的实施例的利用Nuviaq系统的服务开通处理的步骤的例证序列图。图26C中说明的序列图仅仅是例子,并不是对本发明的限制。

[0157] 安装/更新应用使用情况-在确认应用档案满足公共云的安全要求之后,安装应用操作把应用部署到运行中的WebLogic Server。在一个实施例中,提供给安装应用动作的应用部署描述符允许设定变更应用的配置,以满足租户的预订要求的性质。例如,这些性质可包括:

[0158] Property:oracle.cloud.service.weblogic.state

[0159] 值:RUNNING,STOPPED

[0160] 说明:指定部署之后的应用的初始状态。

[0161] 图26D是图解说明按照本发明的实施例的利用Nuviaq系统的部署处理的步骤的例证序列图。图26D中说明的序列图仅仅是例子,并不是对本发明的限制。

[0162] 从而,在一些实施例中,协同工作的TAS 2104和SDI 2106负责为客户从云基础设施系统2000提供的一组服务中定购的一个或多个服务调配资源。例如,在一个实施例中,为了开通数据库服务,对于付费预订,自动化的服务开通流程如下:

[0163] (1)客户通过存储卡UI 2110,发出对于服务的付费预订的定单。

[0164] (2)TAS 2104接收预订定单。

[0165] (3)当服务可用时,TAS 2104通过利用SDI 2106的服务,启动服务开通。TAS 2104可进行商业过程编排,所述商业过程编排将执行有关的商业过程,以完成定单的服务开通方面。在一个实施例中,TAS 2104可利用BPEL(Business Process Execution Language)过程管理器来编排服务开通中涉及的各个步骤,和处理生命周期操作。

[0166] (4)在一个实施例中,为了开通数据库服务,SDI 2106可调用CLOUD_UI中的PLSQL API,以关联用于请求客户的模式。

[0167] (5)在模式和客户的成功关联之后,SDI用信号通知TAS,然后TAS向客户发送客户现在可以应用数据库服务的通知。

[0168] (6)客户可登录到云基础设施系统2000(例如,利用诸如cloud.oracle.com之类的URAL),并启动该服务。

[0169] 在一些实施例中,还可允许客户试用地预订服务。例如,可通过云UI 2112(例如,利用cloud.oracle.com),可以接收这样的试用定单。

[0170] 在一些实施例中,云基础设施系统2000使底层的硬件和服务实例能够在客户或租户之间共享。例如,在一个实施例中,可如图26E中所示,开通数据库服务。图26E描述多个Exadata计算节点2630和2632,每个Exadata计算节点为数据库服务提供调配的数据库实例。例如,计算节点2630为数据库服务提供数据实例2634。每个Exadata计算节点可具有多个数据库实例。

[0171] 在一些实施例中,每个数据库实例可包含多种模式,所述模式可以与不同的客户或租户关联。例如,在图26E中,数据库实例2634提供两种模式2636和2638,每种模式具有它自己的表格。模式2636可以与预订数据库服务的第一客户或租户相关,而模式2638可以与预订数据库服务的第二客户或租户相关。每个租户获得完全隔开的模式。各个模式作用就像可为关联的租户管理数据库对象(包括表格、视图、保存的进程、触发等)的容器。每个模式可具有一个专用表空间,每个表空间具有一个数据文件。

[0172] 按照这种方式,单一数据库实例可向多个租户提供数据库服务。这不仅能够在租户之间实现底层硬件资源的共享,而且能够实现服务实例的共享。

[0173] 在一些实施例中,利用IDM 2100便利这种多租户系统,IDM 2100有利地使都具有各自的单独身份域的多个独立客户能够利用在云中共享的硬件和软件。从而,各个客户不需要具有自己的专用硬件或软件资源,在一些情况下,在特定时刻,未被一些客户使用的资源可被其他客户使用,从而避免这些资源被浪费。例如,如在图26E中所示,数据库实例可服

务都具有各自的相应身份域的多个客户。尽管每个这样的数据库服务实例可以是在多个单独的身份域之间共享的单个物理的多租户数据库系统的单独抽象或视图，不过，每个这样的数据库服务实例可具有单独的并且可能与每个其它数据库服务实例具有的模式不同的模式。从而，多租户数据库系统可保存客户指定的数据库模式和这些数据库模式附属于的身份域之间的映射。多租户数据库系统可使特定身份域的数据库服务实例利用映射到该特定身份域的模式。

[0174] 多租户还可被扩展到诸如Java服务之类的其它服务。例如，多个客户可具有置于他们各自的身份域内的JAVA服务实例。每个这样的身份域可具有可被看作硬件的虚拟“切片”的JAVA虚拟机。在一个实施例中，作业监控服务(例如，Hudson)可以与云中的JAVA企业版平台(例如，Oracle WebLogic)结合，以使各个单独的身份域具有它自己的JAVA企业版平台的独立虚拟“切片”。例如，这种作业监控服务可监控重复作业的执行，比如建立由操作系统的时基作业调度器运行的软件项目或作业。这种重复的作业可包括软件项目的连续建立和/或测试。另外或者另一方面，这种重复的作业可包括监控在机器上执行的操作系统运行的作业的执行，所述机器远离作业监控服务所运行于的机器。

[0175] 如上所述，单一IDM系统可包括多层和多个子系统。概念上，这些子系统中的至少一些子系统可水平地相对于彼此定向，以致概念上，它们位于IDM系统的同层内。不过，IMD系统的不同组件可以位于IDM系统的不同层。在IDM系统的身份数据可被保存在概念上的最底层中。除了其它各种信息以外，身份数据可包括用户身份和定义。身份数据可包括IDM系统已知的所有实体的身份，而不管这些实体限于的特定分区或者身份域。这样的实体可包括与IDM系统交互作用的人。所述实体还可包括非人类系统。

[0176] 保存在身份数据中的身份可被组织成目录。与IDM系统交互作用的各种产品可被配置和设计成知道所述目录。例如，所述产品可包括实现单点登录(SSO)功能的身份管理器和/或访问管理器。在实施例中，尽管IDM系统的所有身份都可被保存在IDM系统的概念上的最底层中，不过，这些身份可被组织成彼此隔离的分区。在一个方面，身份数据可被想象成IDM系统的核心。众多的各种身份管理服务可依赖于通过这种分区实现的隔离。这些身份管理服务可提供租用的抽象。在IDM系统的每个特定层中，存在于该特定层内的子系统可依赖于由存在于下一层内的子系统提供的租用的抽象(最底层除外)，在所述特定层内的子系统可向存在于上一层内的子系统提供租用的抽象(最顶层除外)。

[0177] 本发明的实施例可把单一IDM系统分成多个单独的身份域。IDM系统管理的数据可被身份域分割。属于特定身份域的数据可以与所有其它身份域隔开。如上所述，IDM系统可被多个独立的租户共享。每个这样的租户可以是在IDM系统内为其机构创建了身份域的客户。从而，从安全性的观点看，身份域可被视为隔离的单位。身份域或者租用可为其租户提供安全隔离。在一个实施例中，单个客户可在IDM系统内创建多个单独的身份域或者租用。例如，单个客户可从IDM系统提供者购买专用于测试目的的身份域和专用于生产目的的另一个身份域。

[0178] 在本发明的实施例中，可在知晓身份域映射到身份存储库的方式的情况下，设计利用下层身份存储库的上层子系统。这些上层子系统可从身份存储库接收身份域句柄。这些上层子系统可利用所述身份域句柄创建身份域和身份存储库之间的映射。在IDM系统的各层中，该层内的子系统可以是来自IDM系统的其它各层的信息的消费者。各个子系统可以

利用其身份域句柄来管理和它的身份存储库的分区有关的信息。特定层内的子系统可把其身份域句柄向下传送给在下一层内的子系统，以确保这些子系统将与身份存储库的正确位置交互作用。

[0179] 各个不同的子系统都可在创建多租户IDM系统中扮演角色。例如，SSO子系统可被设计成导致IDM系统内的多个单独SSO部署的出现。每个子系统可包括运行时组件和其中包含其元数据的储存库。每个这样的运行时组件可被设计成与多租户环境中的独立身份域交互作用。

[0180] 应用可类似地被设计成与多租户环境中的独立身份域交互作用。例如，这种环境中的两个不同的应用可以彼此交互作用，这两个应用都是多租户感知的。在这样的情况下，当用户与所述应用中的第一应用交互作用时，第一应用可确定所述用户属于的身份域(从一组身份域中)。在进行了所述确定的情况下，第一应用随后把用户的身份域传送给第二应用。第二应用从而可在获取数据时，在第二应用的储存库内，查询与用户的身份域有关的恰当数据分区。概念上，身份域可被想象成跨是多租户感知的应用实例，关联一段信息。

[0181] 在云计算环境中，一些应用可以是多租户感知的，而其它应用可以不是多租户感知的。这里把不是多租户感知的应用称为“单租户应用”，而把多租户感知的应用称为“多租户应用”。在实施例中，专用于特定身份域的单租户应用的实例可被属于该特定身份域的实体独占使用。例如，Oracle Fusion应用的独立实例可被例示和专用于该应用已被提供给的每个身份域。特定的服务实例可被专用于特定的身份域，以致每个单独的身份域可具有它自己的该特定服务的专用实例。在云计算环境内发生的每个事务可在身份域的上下文中进行，而不管卷入该事务的应用是单租户应用还是多租户应用。

[0182] 图1是按照本发明的实施例，从租户的角度概念地图解说明共享IDM系统100的例子的方框图。共享IDM系统100可包括共享IDM和安全基础设施102，身份域110A、110B和110C中的服务实例，和租户用户112A、112B和112C。特别地，租户A用户112A可利用身份域A 110A中的服务实例，租户B用户112B可利用身份域B 110B中的服务实例，而租户C用户112C可利用身份域C 110C中的服务实例。每个身份域可以与共享IDM系统100中的各个其它身份域隔离，以致每个租户的用户只能够被允许使用在该租户的身份域中的服务实例。如上所述，共享IDM系统100的提供者的特定客户可在云计算环境内创建一个或多个租用或者身份域。

[0183] 共享IDM系统100中的每个身份域可包括单独并且可能不同的一组服务实例。特定的一组服务实例内含在特定的身份域内可以是该特定身份域的客户从共享IDM系统100的提供者购买或租用这些服务实例的使用的结果。与客户在该客户自己的网络中部署应用的方式类似，客户可购买或租用云计算环境内的服务实例的使用；于是可通过并非客户自己拥有或占有的硬件、软件和/或网络提供这样的服务实例。身份域A 110A中的服务实例可包括数据库服务实例116A、JAVA服务实例118A和融合客户关系管理(CRM)服务实例120A。身份域B 110B中的服务实例可包括数据库服务实例116B和JAVA服务实例118B。身份域C 110C中的服务实例可包括数据库服务实例116C、融合CRM服务实例120C和社交网络服务实例122C。尽管一些服务实例实际上可以是各个身份域中的独立的单租户实例，不过，其它服务实例可以是相同的单一多租户服务实例的表现。例如，数据库服务实例116A、116B和116C都可以是相同的单一多租户数据库服务实例的表现。

[0184] 如果特定客户希望特定的一组服务实例与特定的身份域关联，那么该特定客户可

在其购买或租用所述特定的一组服务实例时，向共享IDM系统100的提供者表达该意图。特定的身份域内的(例如用户的)身份都可由该特定身份域的一个或多个身份域管理员集中管理。例如，特定身份域可包括3个不同用户的身份。该特定身份域的身份管理员可指定第一用户可访问特定身份域的服务实例的第一子集，第二用户可访问特定身份域的服务实例的不同的第二子集，第三用户可访问特定身份域的服务实例的仍然不同的第三子集。从而，各个用户可访问都由特定身份域的身份域管理员指定的特定身份域的服务实例的不同子集。

[0185] 在实施例中，特定身份域内的所有服务实例可利用用户身份的相同定义。和典型的企业系统中一样，可以一次创建身份域内的各个用户的身份。包含在身份域内的应用和服务从而可获得关于在该身份域内创建的用户身份的信息。身份域管理员可利用各种技术把用户身份映射到应用和服务。例如，可通过利用角色、分组、规则等，构成这样的映射。在身份域中可以创建具有相关权限和授权的角色。每个角色可以和可被与该角色相关的那些用户访问的一组不同的应用和服务关联。身份域管理员随后可使各个角色与一组不同的用户身份关联，从而准许某些组的身份域的用户访问身份域内的某些组的应用和服务。另一方面，身份域管理员可直接向某些用户身份准许访问定制的一组身份域的应用和服务。在本发明的一个实施例中，角色本身可被格式化和保存为共享IDM系统100的身份存储库内的身份。用户可以与各种不同的角色关联。

[0186] 如上面所述，在一个实施例中，为共享IDM系统100创建的所有身份可被保存在相同的身份存储库内，不过所述身份存储库可被分成不同的“切片”，每个切片与不同的身份域相关。从而，租户A用户112A的身份可在第一切片中，租户B用户112B的身份可在第二切片中，而租户C用户112C的身份可在第三切片中。在本发明的一个实施例中，作为属性，共享IDM系统100的身份存储库中的各个身份可指示该身份属于的身份域。

[0187] 包含在共享IDM系统100中的各个身份域可包括分别表示成Oracle平台安全服务112A、112B和112C的Oracle平台安全服务的对应实例。每个Oracle平台安全服务112A、112B和112C都可以是设计成能够实现对身份信息的访问的应用编程接口(API)的集合。共享IDM和安全基础设施102可包括许多不同的组件，比如身份管理模块104、目录服务和策略存储库106和访问管理模块108。在实施例中，基础设施102内的各个这样的组件实现Oracle平台安全服务112A、112B和112C的API。这些API可向具有各个身份域的服务实例揭示这些服务实例可调用的方法，以便访问和利用基础设施102内的组件。

[0188] 在本发明的实施例中，特定客户首次从共享IDM系统100的提供者购买或租用服务实例时，明确或者隐含地为该客户创建至少一个身份域。另一方面，如果已为特定客户创建和关联了至少一个身份域，那么共享IDM系统100的机构可询问该客户，他是否期望新购买或租用的服务实例被增加到已为该特定客户创建并与之关联的身份域中。如果客户肯定地回答，那么共享IDM系统100可把新购买或租用的服务实例增加到已与现有身份域关联的一组现有服务实例中。按照这种方式，特定客户的服务实例都变成与相同的身份域关联，如果这是该特定客户的意愿的话。例如，这样的服务实例可包括各种SaaS和PaaS实例。

[0189] 在本发明的实施例中，客户可建立与中央存储库的账户，以使客户能够通过中央存储库购买云基服务。当利用该账户通过中央存储库购买服务时，可在云计算环境内，为该客户创建身份域特有的账户。该身份域特有的账户可以和当客户首次通过中央存储库购买

云基服务时，为该客户创建的身份域关联，并与该身份域隔离。从而，可以创建一个账户，以与中央存储库交互作用，可以创建另一个独立的账户，以管理和掌控通过共享IDM系统100创建的身份域。

[0190] 在实施例中，在为客户创建身份域时，客户可指令共享IDM系统100把指定的名称和/或统一资源定位符(URL)绑定到该身份域，以致客户能够区分该身份域和已为相同客户创建的可能的其它身份域。客户及其用户可利用绑定的URL访问云计算环境中的对应身份域及其包含的服务实例。

[0191] 基础设施102的组件不属于为任何客户创建的任何单一身份域。相反，基础设施102可被想象成通常属于云计算环境。然而在本发明的一个实施例中，基础设施102可以与作为整体来看的云计算环境的身份域关联。这种首要的云身份域(也可被称为“操作身份域”)可以与和客户相关的身份域区分开。属于云身份域的用户可被授予访问和管理在客户的任意身份域内的服务实例的特权。这里把这样的用户称为“操作用户”。客户服务代表(CSR)可具有为他们创建的，并与云身份域相关的操作用户身份；于是，云身份域也可被认为是CSR身份域。公共安全模型不仅可以管理身份域的用户与他们的对应身份域的隔离，而且可以便利为集中管理所有身份域所需的交互作用。从而，共享IDM系统100能够阻止与客户的身份域相关的用户对在其身份域外的资源进行操作，但是也能够允许与云域相关的操作用户跨客户的身份域地对资源进行操作。于是，租用的用途至少可以是两方面的：首先，相互隔离租用，其次，管理其它租用(在云身份域的情况下)。

[0192] 图2是按照本发明的实施例，图解说明通过共享IDM系统，为多个客户创建多个身份域的技术200的例子的流程图。尽管技术200被表示成包括按照一定顺序进行的某些操作，不过本发明的备选实施例可包含可能按照不同的顺序进行的另外的，更少的或者备选的操作。在方框202，第一客户通过共享IDM系统，创建第一身份域。在一些实施例中，共享IDM系统保存唯一地定义第一身份域的元数据，以创建第一身份域。在方框204，第一客户通过或者结合共享IDM系统，购买第一组服务实例。在方框206，第一组服务实例中的服务实例被映射到第一身份域。在一些实施例中，共享IDM系统通过创建第一批多个服务和第一身份域之间的映射，使第一批多个服务与第一身份域关联。例如，共享IDM系统可持久地把这样的映射保存在计算机可读存储器内。特别地，如下进一步所述，几个客户都可利用相同的共享IDM系统来建立单独的隔离的身份域，以致不需要按客户例示单独的IDM系统。在方框208，通过共享IDM系统，在第一身份域内，创建第一组用户身份。第一组用户身份中的用户身份被映射到第一身份域。

[0193] 在方框210，第二客户通过共享IDM系统，创建第二身份域。在一些实施例中，共享IDM系统保存唯一地定义第二身份域的元数据，以创建第二身份域。在方框212，第二客户通过或者结合共享IDM系统，购买第二组服务实例。在方框214，第二组服务实例中的服务实例被映射到第二身份域。在一些实施例中，共享IDM系统通过创建第二批多个服务和第二身份域之间的映射，使第二批多个服务与第二身份域关联。例如，共享IDM系统可持久地把这样的映射保存在计算机可读存储器内。从而，几个客户都可利用相同的共享IDM系统来建立单独的隔离的身份域，以致不需要按客户例示单独的IDM系统。在方框216，通过共享IDM系统，在第二身份域内，创建第二组用户身份。第二组用户身份中的用户身份被映射到第二身份域。

[0194] 在方框218，共享IDM系统在第一组服务实例之间，但不在第二组服务实例之间，共享第一组用户身份中的用户身份。在一些实施例中，共享IDM系统至少部分根据按用户的映射，共享第一组用户的身份。在方框220，共享IDM系统在第二组服务实例之间，但不在第一组服务实例之间，共享第二组用户身份中的用户身份。在一些实施例中，共享IDM系统至少部分根据按用户的映射，共享第二组用户的身份。第一组和第二组用户身份都可被保存在相同的共享IDM系统的相同身份存储库中。在方框222，第一身份域的第一身份域管理员利用共享IDM系统，管理第一组用户身份。在方框224，第二身份域的第二身份域管理员利用共享IDM系统，管理第二组用户身份。例如，用户身份的管理可包括增加用户身份、删除用户身份、变更用户身份的属性、增加或删除用户身份和角色和/或分组之间的关联，创建角色和/或分组，向用户、角色和/或分组授予或从用户、角色和/或分组删除服务实例访问许可，等等。在本发明的实施例中，可通过共享IDM系统提供的管理员接口，进行这样的管理。可通过这样的管理员接口，进行各种不同的身份域的管理。从而，共享IDM系统100至少部分根据定义分配给各个用户的一个或多个服务的映射，阻止第一组用户中的用户对在第二组服务中，但不在第一组服务中的服务进行操作。

[0195] 在本发明的实施例中，在共享IDM系统内可规定各种策略。每个这样的策略可包括如果整个策略要被满足，那么必须被满足的一组规则。策略可规定只有当策略的规则都被满足时，才批准对服务实例或系统资源的访问。也可存在隐含策略，所述隐含策略要求为了特定用户可以访问客户的身份域的服务实例，特定用户的身份域必须属于相同的身份域。然而，这种隐含策略可允许可位于任何客户的身份域之外的操作用户访问任何客户的身份域的服务实例。在多租户IDM系统中，可以构思各个策略，以反映与特定身份域相关的服务实例将被隔离在该特定身份域内的意图。

[0196] 例如，云计算环境可包括目录和访问管理系统，比如SSO系统。SSO系统可保护大量的URL。SSO系统可被配置成保护指定的一组URL，但不保护不在所述指定组中的URL(意味后面的这些URL不受保护)。云计算环境内的单一主机可以与多个不同的URL关联。概念上，云计算环境内的每个主机可被设想成竖立在主机和希望访问所述主机的用户之间的多道门。当用户企图访问与特定主机相关的URL时，SSO系统可把该用户路由到适当的主机。保护主机的门可检查在访问该主机的企图中使用的完全合格的URL。所述门可把用户重定向到SSO服务器，或者查寻并强制实施与主机和URL有关的策略。这样的策略可指示用户要被认证，要发现用户的属性，并且根据用户的属性，决定用户是否被允许访问利用该URL的主机。在本发明的实施例中，可以增强这样的策略，以反映由共享IDM系统定义的身份域的边界。

[0197] 图3是按照本发明的实施例，图解说明分层的云基IDM系统300的概况的例子的方框图。云基IDM系统300可包括多层，比如云安全基础层302、云共享IDM层304和Oracle IDM/安全层306。在实施例中，云安全基础层302与云共享IDM层304进行接口，云共享IDM层304与Oracle IDM/安全层306进行接口。Oracle IDM/安全层306可实现“原始”身份管理系统。云共享IDM层304可包括用于隔离各个租户的数据，从而创建支持多个租户和隔离的身份域的概念的“原始”身份系统的抽象的模型。每一层可包括多个子层和子系统，其中的一些将在下面进一步讨论。

[0198] 图4是按照本发明的实施例，图解说明云安全基础层400的子系统的例子的方框图。图4的云安全基础层400可对应于图3的云安全基础层302。安全基础层400可包括多个子

系统，比如租户管理委托模型404，云基础设施生命周期&运行时模型406，操作用户生命周期408，公共策略410，云公钥基础设施(PKI)密钥提供412，和身份和策略存储库的数据安全414。

[0199] 租户管理委托模型404可以是考虑到身份域的体系结构的存在和这些身份域与服务实例的关联的模型。该模型可用于指定与身份域相关的各个用户对于该身份域或其中的元素所具有的角色。该模型可指定向各个角色授予的权限(例如，对于服务实例、用户、角色等)。租户管理委托模型404使购买了身份域的客户能够把某个用户任命为该身份域的身份域管理员。在一个实施例中，这样的客户可以利用云安全基础层400的组件创建角色的层次。可在初始创建身份域时，隐含地创建所述层次，所述层次可以与其创建导致所述层次的创建的身份域具体相关。从而，每个身份域可以与角色的单独并且可能不同的层次相关。在实施例中，隐含地在所述层次的顶部或根部创建的角色是该身份域的身份域管理员的角色。每个身份域可具有一个或多个身份域管理员。身份域管理员可具有足以管理整个身份域，包括所有的服务实例、用户和存在于该身份域内的其它角色的权限和特权。

[0200] 在角色层次中的身份域管理员之下，可以设置服务管理员。尽管这里利用术语“服务管理员”来描述具有管理身份域内的服务实例的权限的角色类别，不过不一定存在称为“服务管理员”的任意角色；相反，可以存在属于“服务管理员”类别的各种具体角色。例如，每种服务实例可具有管理该服务的一类服务管理员角色。服务管理员角色的例子包括JAVA服务管理员，数据库服务管理员，融合应用管理员等等。身份域管理员可利用云安全基础层400的组件把与身份域相关的一个或多个用户任命为服务管理员。由于“服务管理员”可以是角色的类别，而不是角色本身，因此身份域管理员用于把其他用户任命为服务管理员角色的用户接口可列出身份域管理员能够把用户任命成的每种具体类型的服务管理员角色(例如，JAVA服务管理员、数据库服务管理员、融合应用管理员等等)。每个服务管理员可具有为掌控和管理身份域内的特定服务实例所需的权限和特权。每个服务管理员可具有为管理具体与他管理的特定服务实例相关并且范围局限于他管理的特定服务实例的角色所需的权限和特权。然而，特定的服务管理员不一定具有管理任何其它服务实例，或者掌控整个身份域的任何特权。每个服务实例可具有它自己单独的服务管理员。相同的用户可能被任命成相同身份域中的多个服务实例的服务管理员。身份域管理员可进行服务管理员能够进行的所有功能，因为身份域管理员在角色层次中位置较高，但是反过来不成立。在实施例中，在身份域中可为其创建服务实例的各个服务的设计者被赋予确保服务设计者定义的与服务相关的角色的层次一般在其根部包括整个地用于该服务的服务特有的服务管理员角色。

[0201] 图7是按照本发明的实施例，图解说明其中角色层次可用于管理身份域的云基IDM系统700的例子的方框图。图7表示客户(商店账户管理员)702、客户身份域704和云身份域708。客户702不一定实际在任何身份域内。客户702可改为具有在线商店的商店账户。客户702于是是该商店账户的管理员，所述商店账户可以是完全在云基系统之外的账户。客户702可利用该账户购买一个或多个身份域，比如客户身份域704，和购买待部署到这样的身份域中的服务实例。客户702可以购买者的身份行动。由于客户702不一定具有身份域内的用户身份，因此在通过在线商店购买客户身份域704时，客户702可把另一个用户(例如，通过向在线商店指定另一个用户的电子邮件地址)任命成客户身份域704的身份域管理员710

(下面更详细说明)。按照这种方式,具有客户身份域704内的用户身份的用户可访问客户身份域704,即使客户702没有这样的用户身份。

[0202] 客户身份域704包括已被分配在客户身份域704的范围内、未扩展到任何其它身份域的各种角色的用户。上面提及的身份域管理员710的角色可在这些角色之中。身份域管理员710可由客户702任命。身份域管理员702可把作为其角色的一部分,他所具有的至少一些的权限和特权委托给客户身份域704内的其它角色。这些其它角色可包括服务和应用管理员角色,比如身份管理员712、JAVA服务管理员714、数据库服务管理员716和融合应用管理员718。这些服务管理员都可具有(但不限于)为对于客户身份域704内的特定服务实例的用户和角色的掌控和管理所需的权限和特权。

[0203] 身份管理员712可具有在客户身份域704内进行角色管理720和用户管理722的任务的权限。身份管理员712可把角色管理720和用户管理722作为角色委托给客户身份域704内的其它用户身份。借助这些权限,可以管理与客户身份域704有关的用户身份和角色身份(例如,密码重置操作)。身份管理员712可以和身份域管理员710是同一用户。JAVA服务管理员714可具有进行JAVA管理员724的任务的权限。JAVA服务管理员714可把JAVA管理员724作为角色委托给客户身份域704内的其它用户身份。借助这些权限,可以例示、变更和删除JAVA虚拟机。数据库服务管理员716可具有把数据库服务特有的角色分配给客户身份域704内的其他用户的权限。这些数据库服务特有的角色可包括用户726、开发人员728和管理员730的角色。每个这样的角色可具有相对于数据库服务实例的不同权限。例如,用户726可被局限于使用户726能够查询和以其它方式利用保存在数据库的表格中的数据的权限;开发员728可另外具有使开发员728能够变更数据库的配置(比如系统参数)的权限;管理员730可具有进行与数据库服务实例有关的所有动作,包括与该服务实例有关的其他用户的管理的权限。管理员730可以和数据库服务管理员716是相同用户。融合应用管理员718可具有创建和修改CRM层次732,供融合应用实例之用的权限。利用这些权限,融合应用管理员可把具有客户身份域704内的用户身份的用户放入CRM层次732中。融合应用管理员718可具有定义CRM层次732中的各个位置的角色和对应权限的权限,每个这样的角色局限于与融合应用实例有关的操作的执行。也可定义和分派其它服务管理员角色。

[0204] 在一个实施例中,如上所述,由客户702(一般在创建客户身份域704时)指派的身份域管理员710可把权限和服务实例角色委派给客户身份域704内的其它用户。另外,在实施例中,客户702可直接任命客户身份域704内的用户成为具有这些服务实例角色的服务管理员。例如,在实施例中,客户702可直接任命身份域管理员710、身份管理员712、JAVA服务管理员714、数据库服务管理员716和融合应用管理员718中的每一个。在实施例中,作为和服务实例角色有关的服务实例的购买的一部分,客户702可把这些其他用户任命成这些服务实例角色。例如,在购买服务实例的时候,客户702可向从其购买服务实例的在线商店,指定客户702任命为该服务实例的服务实例管理员的用户的一个或多个电子邮件地址。在客户702指定的身份域内,可为具有这些电子邮件地址的用户自动创建用户身份,这些用户可被分派由客户702指定的服务实例的服务管理员角色。

[0205] 此外,如上所述,除了诸如客户身份域704之类的客户身份域之外,云基IDM系统700可包括诸如云身份域708之类的首要云身份域。云身份域708可包括上面说明的操作用户。云身份域708不属于任何客户,独立于任何客户存在。云身份域708中的用户可具有管理

客户身份域，比如客户身份域704(以及存在于云基IDM系统700内的未图示的其它客户身份域)内的角色、用户和服务实例的权限。在云身份域708内，可以定义操作角色层次734。对于云身份域708中的各个操作用户，操作角色层次734可定义该操作用户拥有的权限、特权和角色。在云身份域708内定义的策略可限制某些操作角色可以访问哪些客户身份域，和某些操作角色可对这些客户身份域内的服务、用户和资源进行的操作的种类。例如，云身份域708内的操作用户身份的子集可被角色和/或策略限制于身份管理功能的执行，尽管这些操作用户身份可能具有对在云基环境中的任何客户身份域中定义的身份，进行这样的身份管理功能的能力。在各个身份域中，运行时实例可强制实施这样的策略。

[0206] 在云基IDM系统700中，可以分层地定义角色。层次中的低级角色可以得到的特权和权限可被层次中的高级角色继承。角色层次中的另一个角色的父角色或先辈角色可以继承子角色或后代角色可得到的特权和权限。从而，尽管身份管理员712能够继承角色管理720和用户管理722角色的角色和对应的基于权限的能力，并且身份域管理员710能够继承身份管理员712的角色和对应的基于权限的能力，不过在层次中，继承不能沿相反的方向进行。在实施例中，在服务实例被增加到身份域中时，为各个服务实例自动创建角色层次；角色层次内的角色稍后可由具有分派和/或修改权限的用户分派和/或修改。各个服务实例的角色层次可不同，因为它定义与在其它服务实例的角色层次中定义的角色不同的角色。

[0207] 在实施例中，根据被增加到身份域中的服务实例的种类，在身份域内可自动创建服务实例的预先定义的角色(可能数以千计)；用户不一定需要手动定义各个角色层次中的各个角色。在服务的任意实例被增加到任何身份域中之前，可以使每种类型的服务与可由服务的创始者预先定义、并在服务实例被增加到身份域中时自动创建的服务类型角色层次关联；例如，数据库服务可以与预先定义的数据库服务角色层次关联，JAVA服务可以与预先定义的JAVA服务角色层次关联。从而，每种服务可以与这种服务的分层相关的角色的独立并且可能不同的预定“模板”关联。一些角色，比如身份域管理员710可在整个云的角色模型内预先定义(从而可能具有不变的定义)，而其它服务实例特有的角色可由具有适当权限的那些角色创建和人工定义，以具有和特定服务实例有关的定制权限。

[0208] 与预先定义的服务类型特有的角色层次中的角色相关的权限可被在整个云的模型内定义的层次较高的角色继承。例如，特定类型的服务(例如，数据库服务)的各个服务管理员角色可继承在该特定类型的服务特有的角色层次中预先定义的所有角色(及相关权限)。身份域管理员角色可以继承由身份域中的所有服务管理员角色继承的所有角色(及相关权限)。从而，尽管角色继承使身份域管理员710能够进行任意服务管理员712-718能够进行的任意操作，不过，身份管理员712不一定能够进行其它服务管理员714-718能够进行的操作；身份管理员712可被限制于进行身份域内的基于普通身份的操作，而不是任何特定服务实例特有的操作。由于在身份域之外，在一个实施例中，客户702不继承任何角色。

[0209] 在实施例中，当客户702利用在线商店任命某人具有客户身份域704内的特定角色，比如身份域管理员710或服务管理员712-18任意之一时，在线商店可响应地向被任命者的电子邮件地址发送电子邮件消息。作为任命过程的一部分，客户702把电子邮件地址提供给在线商店。发送给被任命者的电子邮件地址的电子邮件消息可包括指向由云计算环境内的web服务器提供的基于web的表格的超链接。基于web的表格可包括可填写的字段，通过所述字段，消息接收者可指定可用于在客户身份域704内创建被任命者的用户身份的用户名、

密码和其它信息。当被任命者把填写好的基于web的表格提交给web服务器时，web服务器可使被任命者的用户身份在客户身份域704内被创建，并且可使指定的角色被分派给该用户身份。任命可被看作在身份域之外的实体向身份域内的用户身份分派角色的过程，而委托可被看作身份域内的用户身份向在所述用户身份域内的另一个用户身份，分派以前的用户有权(依据他自己在身份域中的角色)分派的角色的过程。

[0210] 图11是进一步图解说明按照本发明的实施例，并且如上所述的多租户IDM系统中的角色委派的方框图。系统1100可包括在线商店1102和客户的身份域1104。客户(商店账户管理员)1106可具有在线商店1102的账户。客户1106可向具有身份域1104内的身份的各个用户任命各种角色，如用图11中的虚线箭头所示。例如，客户1106可把这样的用户任命成身份域管理员1108，和/或不同的服务实例的服务管理员1112和1114。所述任命可在客户1106从在线商店1102购买身份域1104时进行。具有身份域1104内的身份的这些用户又可把各种角色委派给具有身份域1104内的身份的其它用户，如图11中用实线箭头所示。例如，身份域管理员1108中把诸如身份域安全管理员1110、和/或不同的服务实例的服务管理员1112和1114之类角色委派给其他用户。这些其他用户可进一步把角色委派给具有身份域1104内的身份的另外的其他用户。例如，身份域安全管理员1110可把身份域用户/角色管理角色1116委派给其他用户。再例如，一个服务实例的服务管理员1112可把该服务实例的服务实例特有角色1118委派给其他用户。又例如，另一个服务实例的服务管理员1114可把所述另一个服务实例的服务实例特有角色1120委派给其他用户。

[0211] 图12是进一步图解说明按照本发明的实施例，并且如上所述的多租户IDM系统中的权限继承的方框图。系统1200可包括在线商店1202和客户的身份域1204。客户(商店账户管理员)1206可具有在线商店1202的账户。在实施例中，客户1206不继承任何权限，因为客户1206不是身份域1204内的身份。在身份域1204内，身份域安全管理员1210可从身份域用户/角色管理角色1216继承权限。一个服务实例的服务管理员1212可从相同服务实例的服务实例特有角色1218继承权限。另一个服务实例的服务管理员1214可从所述另一个服务实例的服务实例特有角色1220继承权限。身份域管理员1208又可分别从身份域安全管理员1210，和服务管理员1212及1214继承权限。从而，在实施例中，身份域管理员1208可继承管理身份域中的所有服务实例的权限。

[0212] 图5是按照本发明的实施例，图解说明云共享IDM层500的子系统的例子的方框图。图5的云共享IDM层500可对应于图3的云共享IDM层304。云共享IDM层500可包括租户和服务开通自动化API 502、IDM生命周期操作工具504、租户感知IDM组件扩展506和租户隔离数据模型520。租户感知IDM组件扩展506可包括多租户登录用户接口(UI)和认证模式508、云IDM控制台510、身份联合多租户扩展512、云基础设施证书服务514、用户/角色API 516和应用插件模块多租户扩展518。

[0213] 在实施例中，共享IDM系统的每个组件可包括用于其工件的租户隔离构造，以强制实施身份域之间的隔离。每个这样的租户隔离构造可遵循租户隔离数据模型520。例如，访问管理产品可能需要身份管理服务和对应的策略。为了使这些策略对各个用户来说不同、可定制并且独特，每个客户可具有他自己的共享IDM系统的策略存储库的“切片”。从而，在本发明的一个实施例中，共享IDM系统的策略存储库内的策略可被身份域隔开。保存和管理策略的机制可以是租户特有的。租户感知组件扩展506内的各个子系统可遵循租户隔离数

据模型520，以便在身份域中间强制实施隔离。通过遵循租户隔离数据模型520，各个共享IDM产品能够拥有身份域感知特征。

[0214] 例如，通过提供UI字段，多租户登录UI和认证模式508可遵循租户隔离数据模型520，通过所述UI字段，用户能够识别他正在试图访问的特定身份域。这种特征使用户可以登录云计算环境内的特定身份域。多租户登录UI和认证模式508随后可选择特定的身份域，作为将对照其认证用户的身份域。特别地，认证模式可利用特定身份域，以便在查寻与登录过程中提供的用户身份相关的实际密码时，查询正确的分区。尽管无资格的用户身份被要求在身份域内是唯一的，不过，在多个独立的身份域之间，这样的用户身份可能被重复。在本发明的一个实施例中，完全合格的用户身份可指定这些用户身份属于的身份域，并且在多个独立的身份域之间这样的完全合格的用户身份不会被重复。于是，本发明的实施例提供使认证过程是多租户感知的机制。这样的机制可确定用户的身份域，并能够根据该身份域特有的数据来认证用户。

[0215] 在一个实施例中，云IDM控制台510可在遵循租户隔离数据模型520的租户感知组件扩展506之中。云IDM控制台510可被用于改变用户密码，和进行其它用户身份管理功能。云IDM控制台510可包括控件，通过所述控件，能够确定将在其中进行控制台操作的身份域。从而，当身份域管理员利用云IDM控制台510，增加或删除用户身份时，云IDM控制台510能够确定身份域管理员属于的身份域，能够把用户身份的增加或删除仅仅局限于该身份域。

[0216] 租户和服务开通自动化API 502可用于把购买的服务实例提供给为其购买这些服务实例的身份域。IDM生命周期操作工具504可用于把数据(例如，补丁应用)上传到身份域，从身份域下载数据，和使身份域内的数据同步。

[0217] 图6是按照本发明的实施例，图解说明Oracle IDM/安全层600的子系统的例子的方框图。图6的Oracle IDM/安全层600可对应于图3的Oracle IDM/安全层306。Oracle IDM/安全层600可包括Oracle平台安全服务(OPSS)和Oracle web服务管理器(OWSM)602、Oracle因特网目录(OID)604、Oracle身份联合(OID)模块606和Oracle身份管理器(OIM)608。在本发明的实施例中，与共享IDM系统中的各个身份域相关的身份可被保存在OID 604内。OID 604可实现轻量目录存取协议(LDAP)目录。从而，在实施例中，共享IDM系统中的所有用户的所有身份可被保存在由身份域隔开的LDAP目录中。

[0218] 每个身份域的存取控制子系统可以是策略驱动的，因为只有当在该身份域内定义的、并且与受保护服务或资源相关的策略被满足时，才准许对所述受保护服务或资源的存取。各个身份域可具有强制实施在该身份域内定义的策略的运行时实例。在实施例中，所有身份域的所有策略可被保存在整个云的公共策略存储库中，不过该策略存储库可被身份域分割。

[0219] 如上所述，在本发明的实施例中，客户可使身份域在云基环境中被创建，并且可从在线商店购买将在该身份域内可用的一个或多个服务实例。在本发明的实施例中，按照确保将按正确顺序进行服务实例开通操作的方式，定义多租户云基IDM系统的API。一般，对于身份域将进行的第一个操作是云基IDM系统中的该身份域的创建。一种API方法可接收身份域的名称，并判定云基IDM系统内的任何身份域是否已具有该名称。如果目前不存在具有该名称的身份域，那么该API方法可创建该身份域(部分通过保存定义所述身份域的元数据)。不管在调用API方法之前，该身份域是否存在，API方法都可向调用API方法的实体，返回与

命名的身份域有关的信息。所述实体可利用该信息调用API的另外的方法，以进行与命名的身份域有关的操作，比如服务实例增加。

[0220] 图13是按照本发明的实施例，图解说明提供身份域内的服务实例的系统1300的例子的方框图。例证的操作设想其中客户同时购买身份域和用于该身份域的服务实例的情形。例如，服务实例可以是融合CRM的实例。在(A)，全球单实例(GSI)模块1302可把批准的客户定单发送给TAS模块1304。在(B)，TAS模块1304可指令SDI模块1306创建服务实例。在(C)，SDI模块1306可确定其中将创建所述服务实例的身份域本身还未被创建，从而SDI模块1306可向IDM域提供API 1308发送身份域创建请求。响应该请求，IDM域提供API 1308可使客户身份域1310被创建。在(D)，IDM域提供API 1308可向SDI模块1306发送身份域创建响应，身份域创建响应指示身份域被成功创建，并且包括在稍后的与IDM域提供API 1308的事务中，SDI模块1306可用于提到新创建的身份域(客户身份域1310)的链接信息。在(E)，SDI模块1306可向IDM域提供API 1308发送服务实例创建请求。在该请求中，SDI模块1306可把新创建的身份域(客户身份域1310)称作是其中要创建服务实例的身份域。响应该请求，IDM域提供API 1308可创建特定于创建的服务实例的类型(例如，融合CRM应用)的IDM系统1312中的服务实例足迹。在(F)，IDM域提供API 1308可向SDI模块1306发送服务实例创建响应。在(G)，SDI模块1306可在客户身份域1310内，“再水化”创建的服务实例的类型(例如，融合CRM应用)的服务实例种子IDM系统工件1314。这种再水化可涉及创建保存的服务实例的类型的通用“图像”的副本，和生成并保存把服务实例连接到身份域并为所述身份域定制服务实例的链接信息。在(H)，SDI模块1306可向TAS模块1304发送服务实例创建确认响应，该响应指示在客户身份域1310内，服务实例被成功例示。

[0221] 下表1按照本发明的实施例，表示了对于上面参考图13说明的各种云基事件，作为这些事件的一部分，云基多租户IDM系统的不同组件和云基多租户IDM系统内的实体能够相互传送的信息的种类。

[0222] 表1—服务实例-身份域分派

[0223]

Oracle 云事件	TAS=>SDI	SDI=>IDM 域提供 API	IDM	用户
客户获得其在云中的第一个服务	创建服务：身份域名称，身份域管理员姓名和电子邮件，服务管理员域名和电子邮件，	创建身份域：身份域名称，身份域管理员姓名，身份域管理员电子邮件	1)创建身份域 2)创建身份域管理员用户&身份域管理员角色	
		创建服务：身份域名称，服务管理员姓名，服务管理员电子邮件，服务名称	1)创建服务管理员用户 2) 从服务实例类型模板，创建服务角色	
向管理员通知身份域和第一服务实例	通知身份域管理员			身份域管理员接收通知，登录云，重置初始密码，能够管理身份域中的用户&角色

[0224]

的成功提供	通知服务管理员			服务管理员能够把用户分派给第一服务特有角色，能够管理第一服务实例
客户取得其第二个服务实例	创建服务：身份域名称，身份域名称管理员姓名和电子邮件，服务管理员域名和电子邮件	创建服务：身份域名称，服务管理员姓名，服务管理员电子邮件，服务名称	1)创建服务管理员用户 2)从服务实例类型模板，创建服务角色	
向管理员通知第二服务实例的成功提供	通知身份域管理员			身份域管理员被告知新的第二服务实例
	通知服务管理员			服务管理员可把用户分派给第二服务特有角色，能够管理第二服务

[0225] 把服务实例增加到身份域中可涉及云基环境中的一个或多个虚拟机的例示。作为把服务实例增加到身份域中的一部分，可以例示用于该类服务的虚拟机。在一个实施例中，这种虚拟机，或者“服务实例运行时组件”的例示可伴随有确保这样的虚拟机将与适当的身份域关联，或者“连线到”适当的身份域的配置操作。另外，这种虚拟机的例示可伴随有确保这样的虚拟机将与适当的基于策略的边界关联，或者“连线到”所述边界的配置操作。在本发明的一个实施例中，用于创建指定类型的服务实例的API方法是在云基IDM系统内实现的。这种服务实例创建API方法的调用可使云基IDM系统创建可用于建立服务实例虚拟机和适当的身份域之间的关联的句柄。这种句柄可包括诸如适当的身份域的名称、用户名、密码之类的协调信息。服务实例虚拟机可利用这样的用户名和密码来连接到云基IDM系统，可在连接过程中，指定服务实例虚拟机将在其上下文中运行的身份域的名称。服务实例创建API方法可确保句柄指定的用户名和密码不会在为任何其它服务实例虚拟机创建的句柄中被重复，以致用于其它身份域的服务实例的虚拟机不会不适当地连接到除它们自己的身份域之外的身份域。于是，服务实例创建API方法可向调用该方法的实体返回包含为例示服务实例所需的所有数据的信息向量。

[0226] 各个服务实例虚拟机可被提供对在服务实例虚拟机在其上下文中运行的身份域内定义的身份的访问。可以提供这种访问，以致服务实例虚拟机可认证用户，和查寻与身份

域有关的角色。图8是按照本发明的实施例，图解说明其中使应用实例运行时组件可访问在身份域内定义的身份的多租户IDM系统800的方框图。在图解所示的例子中，应用实例运行时组件用于融合(CRM)应用的实例。系统800可包括融合应用服务802、融合中间件804、策略存储库806、身份存储库808和数据库810。融合应用服务802和融合中间件804一起构成融合应用运行时组件。策略存储库806和身份存储库808可被实现成Oracle因特网目录(OID)或者其它LDAP目录。可保存来自各个单独的身份域的策略的策略存储库806可包括策略存储库根节点826，逻辑安全存储库节点824可分层地源于策略存储库根节点826，策略816、818、820和822可分层地源于逻辑安全存储库节点824。策略816、818和820可以与一个身份域，域A有关，而策略822可与另一个身份域，域B有关。策略816和818可和JAVA服务的单独实例有关，而策略820和822可和融合应用服务的单独实例有关。可保存来自各个单独的身份域的身份的身份存储库808可包括LDAP根节点828，各个身份域830的节点可分层地源于LDAP根节点828，和身份域A 832有关的身份以及和身份域B 834有关的身份可分层地源于各个身份域830的节点。数据库810可保存由融合应用服务802和融合中间件804使用的数据，比如融合在线事务处理(OLTP)数据812和模式814(可能包括融合中间件模式和其它数据库模式)。

[0227] 融合应用可以是存在于多租户IDM系统800内的单租户应用的例子。从而，融合应用服务802的特定实例和融合中间件804可特定于特殊的身份域。在这个例子中，它们特定于身份域A。身份存储库808可被构造成LDAP目录树，朝着其叶节点的方向，LDAP目录树包含和多租户IDM系统800中的独立身份域有关的各个独立子树。融合应用运行时组件的身份存储库句柄只指向LDAP身份层次的作为包含和身份域A 832有关的身份的LDAP子树的根节点的节点。从而，融合应用运行时组件的身份存储库句柄只指向专用于身份域A的身份存储库808的“切片”。在图8中，这种指针被表示成源于融合应用运行时组件，并止于LDAP子树832的箭头线。通过在把融合应用服务增加到身份域A时调用API方法，可以建立这种指针。API方法返回的句柄可包含指定在多租户IDM系统800内识别的，并且明确与身份域A关联的特定用户名和密码的凭证。于是，所述凭证可被绑定到与身份域A有关的身份存储库808的适当“切片”或分区。融合应用运行时组件可利用所述特定的用户名和密码访问身份存储库808的适当分区。OID(它可用于实现身份存储库808)内的存取控制可把融合应用运行时组件的可见性仅仅局限于身份存储库808的适当分区，以致融合应用运行时组件不能访问属于除身份域A外的身份域的身份。

[0228] 多租户IDM系统800中的各个单独的服务实例可把与该服务实例有关的它自己的单独一组策略保存在整个云的策略存储库808内。策略存储库808可被构造成包含每个身份域的子树和每个身份域的子树内的服务实例的策略节点的LDAP树。融合应用运行时组件的策略存储库句柄只指向LDAP策略层次的、作为包含与属于身份域A的融合应用运行时实例有关的策略的LDAP子树的根节点的节点。在图8中，该指针被表示成源于融合应用运行时组件，并止于LDAP策略项820的箭头线。通过在把融合应用服务增加到身份域A中时调用API方法，可以建立这样的指针。于是，融合应用运行时组件变成被绑定或“连线”到策略存储库808的特定分区，所述特定分区明确与和属于身份域A的融合应用服务有关的策略相关。从而，当融合应用运行时组件查询策略存储库808时，只可对于融合应用运行时组件被绑定到的策略存储库808的特定分区，进行所述查询。

[0229] 更一般地，在本发明的实施例中，对于各个服务实例运行时组件，存在边界。可以创建分别只针对身份存储库806和策略存储库808的分别与特定服务实例运行时组件的适当身份域和适当服务实例有关的分区的凭证。一旦被创建，这些凭证就可被传送给服务开通系统，以致服务开通系统可把服务实例运行时组件绑定到都可保存云计算环境中的各个身份域中的各个服务实例的数据的身份存储库806和策略存储库808的适当分区。身份存储库806是可以独立于策略存储库808实现的，因为身份不是服务特有的，而策略可以是服务特有的；从而，和各种数据有关的安全边界在范围方面可不同。相同身份域内的多个服务实例可都被绑定到身份存储库806的相同LDAP子树，但是可被分别绑定到策略存储库808的不同LDAP策略项。

[0230] 在实施例中，一个或多个信息存储库，比如身份存储库806可被保存在诸如OID之类的LDAP目录中。这种LDAP目录一般是分层组织的。在实施例中，单个LDAP目录可保存和云基多租户IDM系统内的多个单独的身份域有关的信息。图16是按照本发明的实施例，图解说明云基IDM系统的多租户LDAP目录1600的结构的例子的分层示图。LDAP根节点1602可以是多个节点(比如系统群组节点1604、系统身份节点1606、身份域节点1608和服务模板节点1610的)父节点。系统群组1604可以是代表整个云系统的，而不是特定于身份域的各组身份的节点的父节点。系统群组1604可以是app ID群组的父节点，app ID群组可以把各个应用身份集合到识别的群组中。系统身份1606可以是代表整个云系统的，而不是特定于身份域的各个身份的节点的父节点。系统身份可以是app ID的父节点，app ID可以识别其身份是整个云系统的，而不是特定于身份域的各个应用。身份域1608可以是各个独立身份域，比如客户A身份域1616A、客户B身份域1616B和CSR(或操作)身份域1618的节点的父节点。如上所述，这些身份域节点中的每一个可以是与它们各自的身份域内的角色和身份有关的众多其它节点的父节点。此外，尽管图16表示每个客户(例如A和B)的单一身份域，不过在备选实施例中，每个客户可具有多个独立的身份域。服务模板1610可以是作为不同服务类型的角色层次的根节点的众多节点的父节点。如上所述，不同的服务类型可被映射到预先定义的角色层次，当把所述类型的服务增加到身份域中时，所述预先定义的角色层次可被自动增加到所述身份域中，从而不用用户为所述服务人工创建这样的角色。

[0231] 图17是按照本发明的实施例，图解说明和不同服务类型的角色模板有关的LDAP目录子树的例证结构的层次图。服务上下文模板节点1701可对应于图16的服务模板节点1610。服务上下文模板节点1701可以是不同服务类型的众多节点的父节点。例如，这样的节点可包括JAVA服务节点1702、数据库服务节点1704和Oracle社交网络(OSN)服务节点1706。节点1702-1706分别可以是作为包含所述服务类型的角色节点的子树的根节点的节点的父节点。例如，角色模板节点1708可以是描述具有JAVA服务类型的服务的预定角色的节点的子树的根节点。再例如，角色模板节点1710可以是描述具有数据库服务类型的服务的预定角色的节点的子树的根节点。又例如，角色模板节点1712可以是描述具有OSN服务类型的服务的预定角色的节点的子树的根节点。这些子树由服务的设计者和创建定义，以致这些服务的用户和管理员，比如身份域管理员和服务管理员不需要人工创建这样的角色，尽管他们可把这样的角色分派给在其身份域内的用户。

[0232] 按照本发明的实施例，多租户IDM系统有利地使都具有各自的单独身份域的多个独立客户能够利用在云中共享的硬件和软件。从而，各个客户不需要具有自己的专用硬件

或软件资源，在一些情况下，在特定时刻，未被一些客户使用的资源可被其他客户使用，从而避免这些资源被浪费。例如，多个客户可具有置于他们各自的身份域内的JAVA服务实例。每个这样的身份域可具有可被看作硬件的虚拟“切片”的JAVA虚拟机。对另一个例子来说，在一个实施例中，多个客户可具有置于他们各自的身份域内的数据库服务实例。尽管每个这样的数据库服务实例可以是在多个单独的身份域之间共享的单个物理的多租户数据库系统的单独抽象或视图，不过，每个这样的数据库服务实例可具有单独的并且可能与每个其它数据库服务实例具有的模式不同的模式。从而，多租户数据库系统可保存客户指定的数据库模式和这些数据库模式附属于的身份域之间的映射。多租户数据库系统可使特定身份域的数据库服务实例利用映射到该特定身份域的模式。在一个实施例中，作业监控服务(例如，Hudson)可以与云中的JAVA企业版平台(例如，Oracle WebLogic)结合，以使各个单独的身份域具有它自己的JAVA企业版平台的独立虚拟“切片”。例如，这种作业监控服务可监控重复作业的执行，比如建立由操作系统的时基作业调度器运行的软件项目或作业。这种重复的作业可包括软件项目的连续建立和/或测试。另外或者另一方面，这种重复的作业可包括监控在机器上执行的操作系统运行的作业的执行，所述机器远离作业监控服务所运行于的机器。

[0233] 图14是按照本发明的实施例，图解说明其中可在身份域之间，共享云的硬件和软件资源的多租户云基系统1400的例子的方框图。系统1400可包括Oracle JAVA云服务管理接口1402、应用最终用户1404、Oracle云服务部署基础设施1406、云应用基础1408、和服务开通系统1410。Oracle JAVA云服务管理接口1402可包括各种用户接口，比如基于web的接口和/或命令行接口。这些接口可用于与Oracle云服务部署基础设施1406交互作用。Oracle云服务部署基础设施1406可以与云应用基础1408交互作用。在实施例中，可以利用融合中间件组件，建立云应用基础1408。在实施例中，云应用基础1408可包括Oracle虚拟装配生成器(OVAB)池1410、数据库服务器1412、web层1414、IDM基础设施1416和企业管理器云控制1422。OVAB池1410可包括JAVA云服务集合1412A-N和CRM服务集合1414A-N。依据各个身份域1424A-N的各个JAVA云服务实例1428的服务开通，可以例示这些集合。通过使每个这样的集合与企业管理器云控制1422和web层1414关联，可以针对其相关的JAVA云服务实例1428使所述集合个人化。用于访问各个集合的端点信息可通过电子邮件，被发送给应用终端用户(例如，应用终端用户1404)。IDM基础设施1416可包括目录1418和访问管理模块1420。服务开通系统1410可包括身份域1424A-N和Oracle虚拟机1426。每个身份域1424A-N可包括它自己的IDM/SSO模块1426、JAVA云服务1428、CRM服务1430和数据库服务器1432。Oracle云服务部署基础设施1406和IDM基础设施1416可以与服务开通系统1410进行接口。

[0234] 图15是按照本发明的实施例，图解说明可在云基系统中用于在隔离的客户之间，共享云硬件的虚拟“切片”的JAVA云服务体系结构1500的例子的方框图。体系结构1500可包括JAVA云服务实例1502、Exalogic存储器1504和数据库云服务实例1506。JAVA云服务实例1502可包括多个Exalogic计算节点，比如Exalogic计算节点1508A和1508B。每个Exalogic计算节点可包括Oracle虚拟机(OVM)实例，比如OVM实例1510A和1510B。每个OVM实例可包括受管服务器，比如受管服务器1512A和1512B。每个受管服务器可运行多个单独的应用。受管服务器1512一起构成提供高可用性的客户专用群集1514。Exalogic计算节点1508可以与Exalogic存储器1504进行接口。Exalogic存储器可包含二进制卷1518、配置卷1520和应用

卷1522。数据库云服务实例1506可包括Exadata(Oracle数据库模式-真正应用群集(RAC)节点)1516。在实施例中，可为关于线程死锁和JAVA虚拟机(JVM)崩溃的服务器重启，配置WebLogic节点管理器。WebLogic聚类可用于标准和企业提供。诸如OVM实例1510A-B之类的服务OVM实例可在诸如Exalogic计算节点1508A-B之类的独立Exalogic计算节点上被启动。当一个Exalogic计算节点上的OVM失败时，另一个Exalogic计算节点的OVM可重启前一个Exalogic计算节点上的失败的OVM。数据库云服务实例1506可以采用Oracle RAC单节点结构。

[0235] 图18是按照本发明的实施例，图解说明可用在云基系统中，并且其中在相同数据库实例中可以使用多种模式的数据库云服务多租户体系结构1800的例子的方框图。利用术语解释，数据库实例是共同地起能够进行诸如查询执行和关系数据处理之类操作的数据库服务器作用的一批执行软件过程。传统上，在单一机构的企业环境中，数据库实例具有规定数据库实例保持的所有数据被组织成的关系结构(比如关系表)的格式的单一数据库模式。然而，按照本发明的实施例，托管在云计算环境中的单一数据库实例可保持多个独立并且可能不同的模式-每个单独的身份域(或“租用”)一个模式。有利的是，这种一个数据库实例多种模式的方法允许多个一般无关的客户(即，租户)利用相同的一组执行数据库软件过程(单一数据库实例)，以致不需要按每个客户的身份域，例示这些数据库软件过程的单独实例。

[0236] 体系结构1800可包括多个Exadata计算节点，比如Exadata计算节点1802A-B。Exadata计算节点1802A-B可以是硬件计算机。每个这样的机器可包括一个或多个硬件处理单元(根据软件指定的机器语言指令，进行处理器级的取指令-解码-执行操作)。每个这样的机器可以是由云基服务的提供者拥有和操作的独立服务器计算装置；从而，在实施例中，预订并利用由在Exadata计算节点1802A-B上运行的数据库软件提供的数据库功能的客户并不拥有Exadata计算节点1802A-B，而只是利用在上面执行的软件过程。Exadata计算节点1802A可由一个或多个分组网络通信耦接到Exadata计算节点1802B。在一个实施例中，为了冗余起见，Exadata计算节点1802B起Exadata计算节点1802A的副本的作用；如果Exadata计算节点1802A发生故障，那么客户可自动相对于Exadata计算节点1802B恢复操作，直到Exadata计算节点1802A被恢复为止。

[0237] Exadata计算节点1802A-B都可执行单独的数据库实例，比如数据库实例1804A-B。各个数据库实例1804A-B可以是从相同的数据库软件代码集执行的单独的一批过程。各个数据库实例1804A-B可保持多个独立、隔离并且一般不同的数据库模式。例如，数据库实例1804A可保持数据库模式1806AA-AN，数据库实例1804B可保持数据库模式1806BA-BN。按照本发明的实施例，每个数据库实例的多个数据库模式的这种保持与传统的每个数据库实例一种模式的方法相反。各个数据库模式1806AA-AN可被映射到单独的身份域。各个数据库实例1804A-B可保持规定其数据库模式和这些数据库模式属于的身份域之间的映射的元数据。由这里讨论的共享IDM访问控制提供的隔离机制确保各个身份域的模式只能被与该身份域相关的用户和服务访问和使用。由于数据库实例1804A-B可在身份域之间被共享，而数据库模式1806AA-AN(及其副本1806BA-BN)可专用于各个身份域，并与所有其它身份域隔离，因而可把数据库模式1806AA-AN(及其副本1806BA-BN)替代地称为“数据库服务实例”。从而，按照本发明的实施例，这里对“数据库服务实例”的引用是对模式-数据库实例对，而

不仅仅是数据库实例的引用。

[0238] 每种数据库模式可指定多个单独的关系表。例如，在数据库实例1804A内，数据库模式1806AA可指定关系表1808AAA-1808AAN，而数据库模式1806AN可指定关系表1808ANA-1808ANN。再例如，在数据库实例1804B内，数据库模式1806BA可指定关系表1808BAA-1808BAN，而数据库模式1806BN可指定关系表1808BNA-1808BNN。由于Exadata计算节点1802B可以是Exadata计算节点1802A的副本，因此数据库模式1806BA-BN及其关系表1808BAA-1808BNN可以是数据库模式1806AA-AN及其关系表1808AAA-1808ANN的副本。在Exadata计算节点1802A对数据库模式或关系表作出的变化会自动传送到并在Exadata计算节点1802A被复制。每种数据库模式还可指定单独的一组保存的进程、触发等。

[0239] 体系结构1800还可包括云存储器1810。云存储器1810可由多个可能独立，但是互连的硬件存储设备，比如硬盘驱动器构成。这些存储设备可能可以(但不一定)与Exadata计算节点1802A-B分开并且与Exadata计算节点截然不同。Exadata计算节点1802A-B访问和管理的数据可分布在各个存储设备之间，以致单个计算节点访问和管理的数据的各个部分可分散在多个单独的存储设备之间，和/或以致一个计算节点访问和管理的数据中的至少一些数据可被保存在和另一个计算节点访问和管理的数据相同的存储设备中的至少一些存储设备上。实际上，在一个实施例中，由于Exadata计算节点1802B是Exadata计算节点1802A的副本，因此这些计算节点中的每个都可共享数据库数据的相同拷贝；在这种情况下，尽管诸如执行数据库软件过程之类的计算资源可被复制，不过被这些过程访问和保持的数据记录可在副本之间被共享。构成云存储器810的硬件存储设备可由云服务提供者拥有和操作，如上所述，云服务提供者一般与其数据记录被保存在这些硬件存储设备上的客户分开并且和所述客户截然不同。

[0240] 云存储器1810可保存表空间1812A-N。在实施例中，每个数据库模式具有独立的专用表空间，其中保存符合该数据库模式的数据。例如，表空间1812A可专用于存储符合数据库模式1086AA(和作为其副本的数据库模式1086BA)的数据，表空间1812B可专用于存储符合数据库模式1086AN(和作为其副本的数据库模式1086BN)的数据。在一个实施例中，由于这些表空间只能通过数据库实例1804A-B访问，因此，这里讨论的共享IDM访问控制强加于数据库实例1804A-B的隔离机制足以确保各个表空间1812A-N与各个其它的表空间1812A-N隔离。从而，在实施例中，只有与特定的数据库模式一样，属于相同的身份域的用户和服务实例才被允许(如果策略也授权的话)访问符合该特定数据库模式的任意数据，即使各个表空间1812A-N可能物理地分布和保存在本身不一定严格地专用于各个身份域的独立硬件存储设备之中。换句话说，各个物理存储设备专用于独立的身份域不一定确保表空间1812A-N被分别专用于属于这些身份域的数据库模式。

[0241] 各个表空间1812A-N可保存独立的数据文件。例如，表空间1812A-N可分别保存数据文件1814A-N。数据文件1814A-N中的各个特定数据文件可物理地包含数据记录(例如，关系表各行)，所述数据记录逻辑地包含在由保存该特定数据文件的表空间专用于的数据库模式定义的关系表内。例如，假定表空间1812A专用于数据库模式1806AA，数据文件1814A可物理地包含逻辑地包含在关系表1808AAA-AAN中(并且逻辑地包含在关系表1808AAA-AAN的副本，关系表1808BAA-BAN)中的数据记录。再例如，假定表空间1812B专用于数据库模式1806AN，数据文件1814B可物理地包含逻辑地包含在关系表1808ANA-ANN中(并且逻辑地包

含在关系表1808ANA-ANN的副本，关系表1808BNA-BNN)中的数据记录。

[0242] 图19是按照本发明的实施例，图解说明Nuviaq云系统1900的例子的方框图。系统1900可包括租户服务开通系统(SDI)1902、租户控制台1904、集成开发环境(IDE)1906、命令行接口(CLI)1908、web门1910、Nuviaq代理1912、Nuviaq管理器1918、Nuviaq数据库1924、平台实例1926、病毒扫描模块1934、IDM系统1936、CRM模块1942和身份管理1940。Nuviaq代理1912、Nuviaq管理器1918和Nuviaq数据库1924一起概念地构成Nuviaq 1950。租户服务开通API 1902和租户控制台1904可与Nuviaq代理1912进行接口。IDE 1906和CLI 1908可与Nuviaq管理器1918进行接口。Web门1910可与平台实例1926进行接口。Nuviaq管理器1918可与Nuviaq数据库1924、病毒扫描模块1934、IDM系统1936和平台实例1926进行接口。平台实例1926可与CRM模块1942和身份管理1940进行接口。Nuviaq代理1912可包括Oracle超文本传送协议服务器(OHS)1914和Web Logic服务器1916A-N。Nuviaq管理器1918可包括OHS 1920和Web Logic服务器1922A-N。平台实例1926可包括Web Logic服务器1928A-N、Web Logic管理服务器1930和实例数据库1932。

[0243] 在实施例中，Nuviaq管理器1918可以充当进入系统1900的入口点。作为这样的入口点，Nuviaq管理器1918可通过安全web服务API，提供对PaaS操作的安全访问。Nuviaq管理器1918可跟踪Nuviaq数据库1924中的系统1900的状态。Nuviaq管理器1918可控制作业执行。租户服务开通系统(SDI)1902可访问Nuviaq管理器1918，以指令Nuviaq管理器1918在云基计算环境中，进行服务开通操作(例如，服务实例提供操作)。租户控制台1914可访问Nuviaq管理器1918，以指令Nuviaq管理器1918在云基计算环境中进行部署操作(例如，服务实例部署操作)。Nuviaq管理器1918可异步地执行涉及这样的操作的作业。这样的作业可涉及特定于PaaS工作流的动作序列。Nuviaq管理器1918可顺序地进行作业的动作。所述动作可涉及把任务委派给其它组件，比如企业管理器(EM)模块的命令行接口。可在连同OHS 1920的Web Logic服务器1920A-N的群集上执行Nuviaq管理器1918。

[0244] 在实施例中，Nuviaq代理1912可以是其它系统可经API与之进行接口的接入点。Nuviaq代理1912可通过所述API，接收来自其它系统的请求，并把这些请求转发给Nuviaq管理器1918。在一个实施例中，Nuviaq代理1912可以位于防火墙之外，而Nuviaq管理器1918位于所述防火墙之内。可在连同OHS 1914的Web Logic服务器1916A-N的群集上执行Nuviaq代理1912。

[0245] 在实施例中，Nuviaq数据库1924可跟踪与平台实例1926，以及部署计划、应用、Web Logic域、作业和报警有关的数据。保存在Nuviaq数据库1924内的主键可以与保存在整个云的服务数据库(未图示)内的关键字对准，所述整个云的服务数据库包含客户(或“租户”)与他们的身份域(或“租用”)及这些客户预订的服务实例之间的映射。

[0246] 在实施例中，平台实例1926为特定身份域提供Web Logic服务资源。从而，可以为云基环境中的各个单独的身份域例示独立的平台实例1926，并且所述独立的平台实例1926专用于云基环境中的各个单独的身份域。然而，各个这样的平台实例1926可由Nuviaq管理器1918集中管理，以致仅仅需要例示Nuviaq管理器1918的不多于一个的实例。在实施例中，Nuviaq管理器1918是为各个身份域创建每个单独的平台实例1926的组件。平台实例1926可被想象成是Web Logic服务器的身份域专用“切片”。Nuviaq 1950处理的一些工作流可涉及对上述服务数据库的访问，以便把Web Logic“切片”配置成充当如由保存在服务数据库内

的映射指示的客户已预订的各个其它服务实例的客户端。租户控制台1904可向在身份域内任命的管理员，提供使这些管理员能够管理在包含在身份域内的平台实例1926上运行的应用的用户接口。CLI 1908也可被用于管理这样的应用。每个平台实例1926可被给予在云计算环境内唯一的标识符，所述唯一的标识符可用于在利用平台实例1926的操作中，引用所述平台实例1926。

[0247] 在实施例中，Nuviaq 1950可以和在Nuviaq 1950之外的组件一道工作，以便进行Web Logic工作流。在这些外部组件之中，租户服务开通模块(SDI)1902可包括集合部署器子系统。集合部署器子系统可管理Nuviaq 1950、Oracle虚拟装配生成器(OVAB)和Oracle虚拟机(OVM)之间的交互作用。Nuviaq 1950可利用集合部署器子系统部署集合、解除部署集合、描述集合部署和缩放设备。Nuviaq 1950可通过web服务API，访问集合部署器子系统。

[0248] 另外在外部组件之中，在允许各种工件被部署到云计算环境中的任意应用之前，病毒扫描模块1934可针对病毒和其它有害的可执行指令，扫描这些工件。病毒扫描模块1934可为云计算环境中的多个独立组件，提供“扫描即服务”。在一个实施例中，病毒扫描模块1934可向多个单独身份域内的组件提供其服务，以致不需要按身份域例示单独的病毒扫描模块。其细节已在上面说明的IDM系统1936可向Nuviaq 1950进行的作业提供安全性。CRM模块1942可以与已被放入各个身份域内的JAVA服务实例关联。这些JAVA服务实例和CRM模块1942之间的这种关联使由所述JAVA服务实例执行的应用能够通过对CRM模块1942发出web服务调用，实现CRM模块1942的CRM功能。

[0249] 硬件概况

[0250] 图9是图解说明按照本发明的实施例可使用的系统环境900的组件的简化方框图。如图所示，系统环境900包括一个或多个客户端计算设备902、904、906、908，所述客户端计算设备902、904、906、908被配置成运行包括本地客户端应用，可能还有诸如web浏览器之类的其它应用的客户端应用。在各个实施例中，客户端计算设备902、904、906、908可与服务器912交互作用。

[0251] 客户端计算设备902、904、906、908可以是通用个人计算机(例如，包括运行各种版本的Microsoft Windows和/或Apple Macintosh操作系统的个人计算机和/或膝上型计算机)，蜂窝电话机或PDA(运行诸如Microsoft Windows Mobile之类的软件，并且允许因特网、电子邮件、SMS、Blackberry或其它通信协议)，和/或运行各种可从市场获得的UNIX或UNIX似的操作系统(包括(但不限于)各种GNU/Linux操作系统)任意之一的工作站计算机。另一方面，客户端计算设备902、904、906和908可以是能够通过网络(例如，下面说明的网络910)通信的任何其它电子设备，比如精简型客户端计算机，允许因特网的游戏系统，和/或个人消息接发设备。尽管例证的系统环境900被表示成具有4个客户端计算设备，不过可以支持任意数目的客户端计算设备。诸如传感器之类的其它设备可以与服务器912交互作用。

[0252] 系统环境900可包括网络910。网络910可以是本领域的技术人员熟悉的可利用各种可从市场获得的协议，包括(但不限于)TCP/IP、SNA、PX、AppleTalk等任意之一，支持数据通信的任意种类的网络。仅仅作为例子，网络910可以是诸如以太网、令牌环网络之类的局域网(LAN)；广域网；虚拟网络，包括(但不限于)虚拟专用网(VPN)；因特网；企业内部网；外联网；公共交换电话网(PSTN)；红外网络；无线网络(例如，按照IEEE 802.11协议组，本领域已知的蓝牙协议，和/或任何其它无线协议任意之一运行的网络)；和/或这些和/或其它网

络的任何组合。

[0253] 系统环境900还包括一个或多个服务器计算机912，所述服务器计算机912可以是通用计算机、专用服务器计算机(例如，包括PC服务器、UNIX服务器、中程服务器、大型计算机、机架安装服务器等)、服务器群、服务器群集、或者任何其它适当的排列和/或组合。在各个实施例中，服务器912可适合于运行一个或多个服务或软件应用。

[0254] 服务器912可以运行操作系统，包括上述那些操作系统任意之一，以及任何可从市场获得的服务器操作系统。服务器912还可运行任何各种另外的服务器应用和/或中间层应用，包括HTTP服务器、FTP服务器、CGI服务器、JAVA服务器、数据库服务器等。例证的数据库服务器包括(但不限于)可在市场上从Oracle、Microsoft、Sybase、IBM等获得的那些数据库服务器。

[0255] 系统环境900还可包括一个或多个数据库914、916。数据库914、916可在各个位置。例如，数据库914、916中的一个或多个可在服务器912本地(和/或在服务器912中)的非临时性存储介质上。另一方面，数据库914、916可远离服务器912，通过网络或专用连接，与服务器912通信。在一组实施例中，数据库914、916可在本领域的技术人员熟悉的存储区域网(SAN)中。类似地，可酌情在服务器912本地和/或远程保存用于实现被认为是服务器912所有的功能的任何必需文件。在一组实施例中，数据库914、916可包括适合于响应SQL格式化命令，保存、更新和取回数据的关系数据库，比如Oracle提供的数据库。

[0256] 图10是按照本发明的实施例可使用的计算机系统1000的简化方框图。例如，可利用诸如系统1000之类的系统，实现服务器912或客户端902、904、906或908。计算机系统1000被表示成包含可通过总线1024，电耦接的硬件元件。硬件元件可包括一个或多个中央处理器(CPU)1002、一个或多个输入设备1004(例如，鼠标、键盘等)，和一个或多个输出设备1006(例如，显示设备、打印机等)。计算机系统1000还可包括一个或多个存储设备1008。例如，存储设备1008可包括诸如磁盘驱动器、光存储设备、和可编程、可闪速更新等的诸如随机存取存储器(RAM)和/或只读存储器(ROM)之类固态存储设备之类的设备。

[0257] 计算机系统1000另外可包括计算机可读存储介质读取器1012，通信子系统1014(例如，调制解调器、网卡(无线或有线)、红外通信设备等)，和工作存储器1018，工作存储器1018可包括如上所述的RAM和ROM。在一些实施例中，计算机系统1000还可包括处理加速单元1016，它可包括数字信号处理器(DSP)、专用处理器等。

[0258] 计算机可读存储介质读取器1012可进一步连接到计算机可读存储介质1010，计算机可读存储介质1010共同(并且视情况，与存储设备1008结合)全面地代表用于临时和/或更长久地包含计算机可读信息的远程、本地、固定和/或可拆卸存储设备加上存储介质。计算系统1014可允许与网络910和/或上面关于系统环境900说明的任何其它计算机交换数据。

[0259] 计算机系统1000还可包括表示成目前位于工作存储器1018内的软件元件，包括操作系统1020和/或其它代码1022，比如应用程序(可以是客户端应用，Web浏览器，中间层应用，RDBMS等)。在例证实施例中，工作存储器1018可包括用于如上所述的多租户云基IDM系统的可执行代码和相关的数据结构。应理解计算机系统1000的备选实施例可具有源于上面所述的众多变化。例如，也可使用定制的硬件，和/或可用硬件、软件(包括可移植软件，比如Java程序)或者这两者，实现特殊的元件。此外，可以采用与诸如网络输入/输出设备之类的

其它计算设备的连接。

[0260] 用于包含代码或代码的各个部分的存储介质和计算机可读介质可包括本领域中已知或使用的任何适当介质，包括存储介质和通信介质，比如(但不限于)利用信息(比如计算机可读指令、数据结构、程序模块或其它数据)的任何存储和/或传输方法或技术实现的易失性和非易失性(非临时性)、可拆卸和不可拆卸介质，包括RAM、ROM、EEPROM、闪存或其它存储技术、CD-ROM、数字通用光盘(DVD)或其它光存储器、盒式磁带、磁带、磁盘存储器或其它磁存储设备、数据信号、数据传输、或可用于保存或传送期望的信息，并且可被计算机访问的任何其它介质。

[0261] 图27、28和29分别表示按照如上所述的本发明的原理构成的计算设备2700、2800、2900的功能方框图。计算设备的功能块可用硬件、软件或者硬件和软件的组合实现，以实现本发明的原理。本领域的技术人员明白，图27、28和29中所示的功能块可被组合，或者分离成子块，以实现如上所述的本发明的原理。于是，这里的说明可支持任何可能的组合或分离，或者这里说明的功能块的另外的定义。

[0262] 如图27中所示，计算设备2700包含第一创建单元2702、第一关联单元2704、第一共享单元2706、第二创建单元2708、第二关联单元2710和第二共享单元2712。

[0263] 第一创建单元2702可通过共享身份管理系统，创建第一身份域。第一关联单元2704可使第一批多个服务与第一身份域关联。第一共享单元2706可在第一批多个服务之间，共享由共享身份管理系统管理的第一组用户的身份。通过共享身份管理系统，第二创建单元2708可创建与第一身份域隔离的第二身份域。第二关联单元2710可使第二批多个服务与第二身份域关联。第二共享单元2712可在第二批多个服务之间，共享由共享身份管理系统管理的第二组用户的身份。

[0264] 计算设备2700还可包括第一和第二映射单元2714和2716。第一映射单元2714可通过共享身份管理系统，把(a)第一组用户中的第一用户映射到(b)对于第一批多个服务的子集的第一访问权限。第二映射单元2716可通过共享身份管理系统，把(c)第二组用户中的第二用户映射到(d)对于第二批多个服务的子集的第二访问权限。

[0265] 计算设备2700还包括第三和第四映射单元2718和2720。第三映射单元2718可通过共享身份管理系统，把(a)第一组用户中的第一用户映射到(b)第一角色，所述第一角色被映射到对于第一批多个服务的子集的第一访问权限。第四映射单元2720可通过共享身份管理系统，把(c)第二组用户中的第二用户映射到(d)第二角色，所述第二角色被映射到对于第二批多个服务的子集的第二访问权限。

[0266] 计算设备2700还可包括第一和第二阻止单元2722、2724和允许单元2726。第一阻止单元2722阻止第一组用户中的用户进行与在第二组服务之中、但不在第一组服务之中的服务有关的操作。第二阻止单元2724阻止第二组用户中的用户进行与在第一组服务之中、但不在第二组服务之中的服务有关的操作。允许单元2726允许用户进行与在第一组服务中的服务和在第二组服务中的服务有关的操作。

[0267] 计算设备2700还可包括把第一组用户的身份保存在由身份域分隔的轻量存取协议(LDAP)目录的第一分区内的第一存储单元2728，和把第二组用户的身份保存在LDAP目录的第二分区内的第二存储单元2730。

[0268] 计算设备2700还可包括呈现包括用户接口元素的用户接口的第一呈现单元2732，

通过所述用户接口元素，作为登录过程的一部分，特定用户能够识别所述特定用户正在试图访问的特定身份域。

[0269] 计算设备2700还可包括呈现控制台的第二呈现单元2734，所述控制台提供用于把用户身份增加到身份域中和从身份域中删除用户身份的控件，通过控制台，从身份域管理员接收命令的第一接收单元2736，确定身份域管理员属于的特定身份域的确定单元2738，和把身份域管理员通过控制台进行的用户身份增加和删除操作局限于所述特定身份域的限制单元2740。

[0270] 计算设备2700还可包括第一、第二和第三分配单元2742、2744和2746。第一分配单元2742可向第一组用户中的第一用户分配身份域管理员角色，所述身份域管理员角色给予第一用户向第一组用户中的其他用户分配服务管理员角色的能力。第二分配单元2744可向由作为身份域管理员的第一用户选择的第一组用户中的第二用户，分配第一服务管理员角色，所述第一服务管理员角色给予第二用户管理第一批多个服务中的第一服务的能力。第三分配单元2746可向由作为身份域管理员的第一用户选择的第一组用户中的第三用户，分配第二服务管理员角色，所述第二服务管理员角色给予第三用户管理第一批多个服务中的第二服务的能力。

[0271] 计算设备2700还可包括：从在第一身份域中无用户身份、但是与购买第一身份域的账户相关的第一人，接收在第一身份域中也没有用户身份的第二人的电子邮件地址的第二接收单元2748；从所述第一人接收在第一身份域内所述第一人任命第二人担任的角色的第三接收单元2750；向第二人的电子邮件地址发送电子邮件消息的发送单元2752，所述电子邮件消息包含到基于web的表格的超链接，所述表格可用于在第一身份域内创建用户身份；根据第二人通过基于web的表格提供的信息，把第二人的身份增加到第一组用户的身份中的第一增加单元2754；和把所述角色分配给第一身份域内的第二人的身份的第四分配单元2756。

[0272] 计算设备2700还可包括：接收把特定服务增加到第一组服务中的请求的第四接收单元2758；响应所述请求，把所述特定服务增加到第一组服务中的第二增加单元2760；和在第一身份域内，定义根据所述特定服务的类型，从角色的多个层次中自动选择的角色的层次的定义单元2762。

[0273] 计算设备2700还可包括：绑定特定服务实例和身份存储库的第一分区的第一绑定单元2764，所述特定服务实例是第一组服务中的服务的实例，所述身份存储库保存在云计算环境中定义的多个身份域的身份；和绑定特定服务实例和策略存储库的第二分区的第二绑定单元2766，所述策略存储库保存关于属于在云计算环境中定义的不同身份域的多个服务实例的策略，其中第一分区只包含属于第一身份域的身份，其中第二分区只包含和特定服务实例有关的策略。

[0274] 参见图28，计算设备2800包括创建单元2802，强制实施单元2804，增加单元2806，第一存储单元2808和第二存储单元2810。创建单元2002在云计算环境内，创建多个身份域。强制实施单元2804可在所述多个身份域内，强制实施身份域之间的隔离。增加单元2806把服务实例增加到所述多个身份域中的特定身份域中。第一存储单元2808保存使服务实例和身份存储库的特定分区相关联的数据，所述身份存储库保存所述多个身份域中的每个身份域的身份。第二存储单元2810保存使服务实例和策略存储库的特定分区相关联的数据，所

述策略存储库保存关于与所述多个身份域中的不同身份域相关的多个服务实例的策略。

[0275] 计算设备2800还可包括第一分配单元2812和第二分配单元2814。第一分配单元2812可把角色的层次中的第一角色分配给第一用户，所述第一用户具有保存在身份存储库中并且与特定身份域相关的第一用户身份。第一角色是允许具有第一角色的用户管理与所述特定身份域相关的所有服务实例的角色。第二分配单元2814可把所述角色的层次中的第二角色分配给第二用户，所述第二用户具有保存在身份存储库中的第二用户身份。第二角色是允许具有第二角色的用户管理与所述特定身份域相关的单一服务实例的角色。

[0276] 在例子中，第二分配单元2814可响应第一用户把第二角色委派给第二用户，把第二角色分配给第二用户。

[0277] 在例子中，增加单元2806还可包括向第三用户分配第三角色的第三分配单元2816，所述第三用户具有保存在身份存储库中并且与所述特定身份域相关的第三身份，所述第三角色由与特定服务实例的类型相关的多个角色定义。

[0278] 计算设备2800还可包括第一继承单元2818和第二继承单元2820。第一继承单元2818可使第二角色继承与第三角色相关的所有权限。第二继承单元2820可使第一角色继承被第二角色继承的所有权限。

[0279] 在例子中，创建单元2802可在云计算环境内，创建特定身份域。这种情况下，创建单元2802还可包括向指定的电子邮件地址，发送电子邮件消息的发送单元2822，所述电子邮件消息提供一种机制，借助所述机制，电子邮件消息的收件人能够在所述特定身份域内，建立管理身份。

[0280] 参见图29，计算设备2900包括建立单元2902、第一提供单元2904和第二提供单元2906。建立单元2902可导致在云计算环境中，建立单一身份管理(IDM)系统。第一提供单元2904可使所述单一IDM系统向与第一身份域相关的第一服务实例提供IDM功能，所述第一身份域是在云计算环境内定义的并且与在云计算环境内定义的第二身份域隔离。第二提供单元2906可使所述单一IDM系统向与第二身份域相关的第二服务实例提供IDM功能。

[0281] 计算设备2900还可包括第一和第二存储单元2908、2910和第一和第二生成单元2912、2914。第一存储单元2908可使单一IDM系统把与第一身份域相关、但是不与第二身份域相关的用户身份保存在维持于云计算环境内的单一身份存储库内。第二存储单元2910可使单一IDM系统把与第二身份域相关、但是不与第一身份域相关的用户身份保存在所述单一身份存储库内。第一生成单元2912使单一IDM系统生成第一凭证，所述第一凭证允许第一服务实例与所述单一身份存储库的包含和第一身份域相关的用户身份的一部分交互作用，但不允许第一服务实例与所述单一身份存储库的包含和第一身份域不相关的用户身份的各个部分交互作用。第二生成单元2914使单一IDM系统生成第二凭证，所述第二凭证允许第二服务实例与所述单一身份存储库的包含和第二身份域相关的用户身份的一部分交互作用，但不允许第二服务实例与所述单一身份存储库的包含和第二身份域不相关的用户身份的各个部分交互作用。

[0282] 计算设备2900还可包含第三和第四存储单元2916、2918和第三和第四生成单元2920、2922。第三存储单元2916可使单一IDM系统把与第一服务实例相关、但是不与第二服务实例相关的安全访问策略保存在维持于云计算环境内的单一策略存储库内。第四存储单元2918可使单一IDM系统把与第二服务实例相关、但是不与第一服务实例相关的安全访问

策略保存在所述单一策略存储库内。第三生成单元2920可使单一IDM系统生成第一凭证，所述第一凭证允许第一服务实例与所述单一策略存储库的包含和第一服务实例相关的安全访问策略的一部分交互作用，但不允许第一服务实例与所述单一策略存储库的包含和第一服务实例不相关的安全访问策略的各个部分交互作用。第四生成单元2922可使单一IDM系统生成第二凭证，所述第二凭证允许第二服务实例与所述单一策略存储库的包含和第二服务实例相关的安全访问策略的一部分交互作用，但不允许第二服务实例与所述单一策略存储库的包含和第二服务实例不相关的安全访问策略的各个部分交互作用。

[0283] 尽管说明了本发明的具体实施例，不过众多的修改、变更、备选结构和等同物也包含在本发明的范围内。本发明的实施例并不局限于在某些特定的数据处理环境内的操作，相反，能够自由地在多个数据处理环境内工作。另外，尽管利用特定的一系列事务和步骤，说明了本发明的实施例，不过对本领域的技术人员来说，本发明的范围显然并不限于说明的一系列事务和步骤。

[0284] 此外，尽管利用硬件和软件的特定组合，说明了本发明的实施例，不过应认识到硬件和软件的其它结合也在本发明的范围内。本发明的实施例可只用硬件实现，只用软件实现，或者可以利用硬件和软件的组合来实现。

[0285] 此外，在功能上，可如下定义本发明的一些实施例。具体地，提供一种包括云计算环境内的单一身份管理(IDM)的系统。所述系统包括向与第一身份域相关的第一服务实例提供IDM功能的装置，所述第一身份域是在云计算环境内定义的并且与在云计算环境内定义的第二身份域隔离；和向与第二身份域相关的第二服务实例提供IDM功能的装置。

[0286] 最好，所述系统还包括把与第一身份域相关、但是不与第二身份域相关的用户身份保存在维持于云计算环境内的单一身份存储库内的装置，把与第二身份域相关、但是不与第一身份域相关的用户身份保存在所述单一身份存储库内的装置，生成第一凭证的装置，所述第一凭证允许第一服务实例与所述单一身份存储库的包含和第一身份域相关的用户身份的一部分交互作用，但不允许第一服务实例与所述单一身份存储库的包含和第一身份域不相关的用户身份的各个部分交互作用，和生成第二凭证的装置，所述第二凭证允许第二服务实例与所述单一身份存储库的包含和第二身份域相关的用户身份的一部分交互作用，但不允许第二服务实例与所述单一身份存储库的包含和第二身份域不相关的用户身份的各个部分交互作用。

[0287] 最好，所述系统还包括把与第一服务实例相关、但是不与第二服务实例相关的安全访问策略保存在维持于云计算环境内的单一策略存储库内的装置，把与第二服务实例相关、但是不与第一服务实例相关的安全访问策略保存在单一策略存储库内的装置，生成第一凭证的装置，所述第一凭证允许第一服务实例与所述单一策略存储库的包含和第一服务实例相关的安全访问策略的一部分交互作用，但不允许第一服务实例与所述单一策略存储库的包含和第一服务实例不相关的安全访问策略的各个部分交互作用，和生成第二凭证的装置，所述第二凭证允许第二服务实例与所述单一策略存储库的包含和第二服务实例相关的安全访问策略的一部分交互作用，但不允许第二服务实例与所述单一策略存储库的包含和第二服务实例不相关的安全访问策略的各个部分交互作用。

[0288] 从而，说明书和附图应被视为对本发明的举例说明，而不是对本发明的限制。不过，显然可对其作出增减、删除和其它修改及变化，而不脱离本发明的精神和范围。

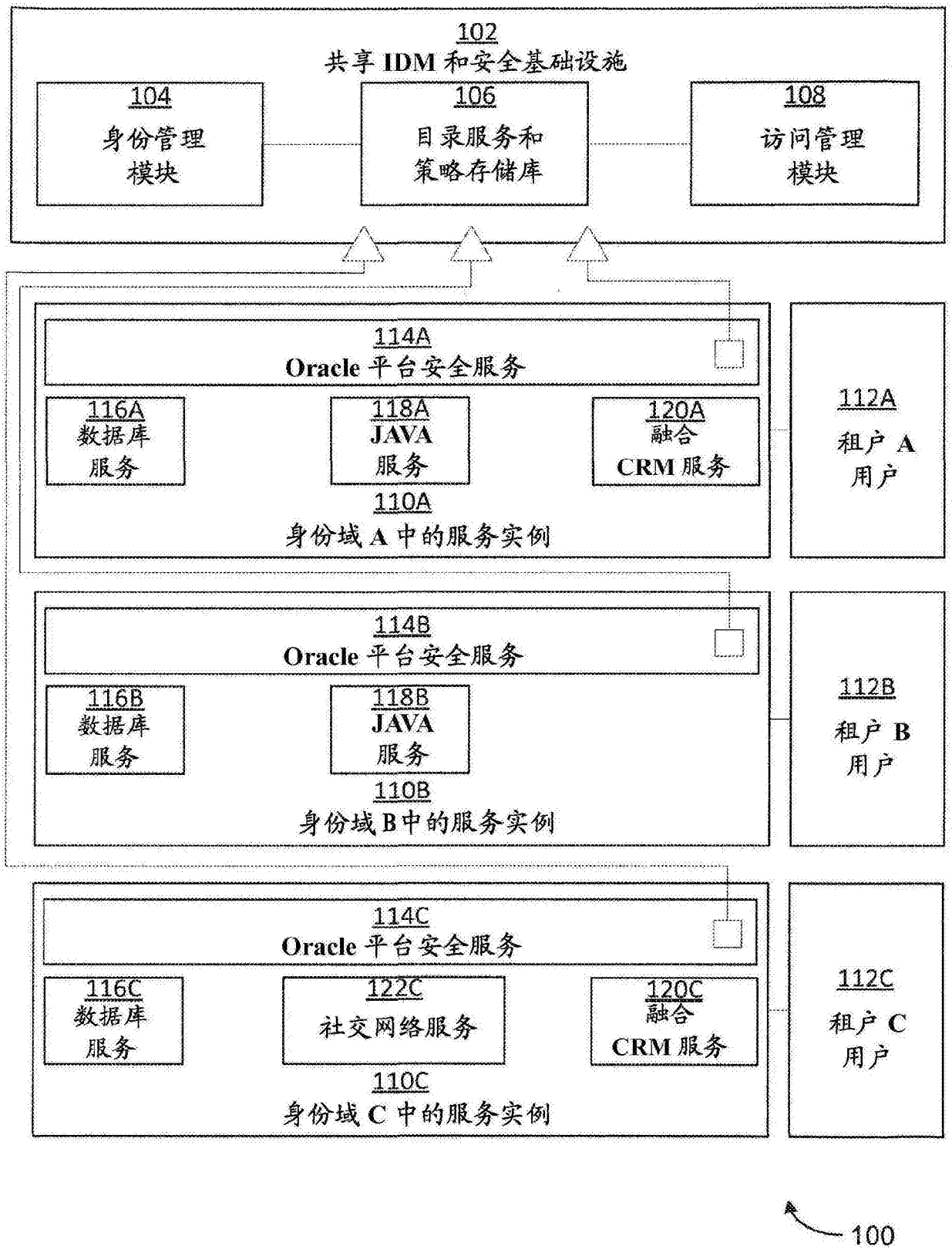

102
共享 IDM 和安全基础设施
104
身份管理
模块
106
目录服务和
策略存储库
108
访问管理
模块
114A
Oracle 平台安全服务
116A
数据库
服务
118A
JAVA
服务
120A
融合
CRM 服务
110A
身份域 A 中的服务实例
112A
租户 A
用户
114B
Oracle 平台安全服务
116B
数据库
服务
118B
JAVA
服务
110B
身份域 B 中的服务实例
112B
租户 B
用户
114C
Oracle 平台安全服务
116C
数据库
服务
122C
社交网络服务
120C
融合
CRM 服务
110C
身份域 C 中的服务实例
112C
租户 C
用户
100

图1

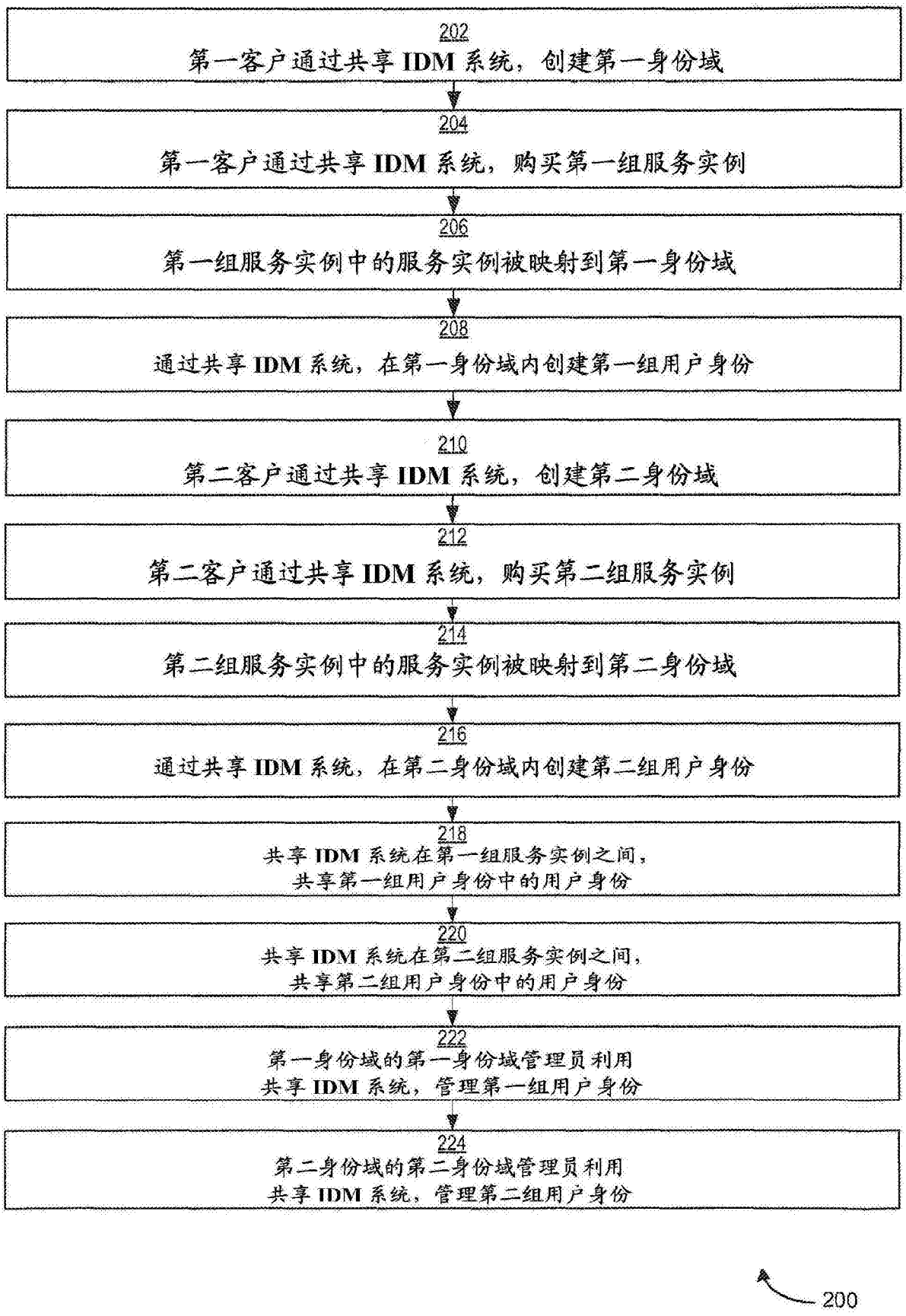

202
第一客户通过共享 IDM 系统，创建第一身份域
204
第一客户通过共享 IDM 系统，购买第一组服务实例
206
第一组服务实例中的服务实例被映射到第一身份域
208
通过共享 IDM 系统，在第一身份域内创建第一组用户身份
210
第二客户通过共享 IDM 系统，创建第二身份域
212
第二客户通过共享 IDM 系统，购买第二组服务实例
214
第二组服务实例中的服务实例被映射到第二身份域
216
通过共享 IDM 系统，在第二身份域内创建第二组用户身份
218
共享 IDM 系统在第一组服务实例之间，
共享第一组用户身份中的用户身份
220
共享 IDM 系统在第二组服务实例之间，
共享第二组用户身份中的用户身份
222
第一身份域的第一身份域管理员利用
共享 IDM 系统，管理第一组用户身份
224
第二身份域的第二身份域管理员利用
共享 IDM 系统，管理第二组用户身份
200

图2

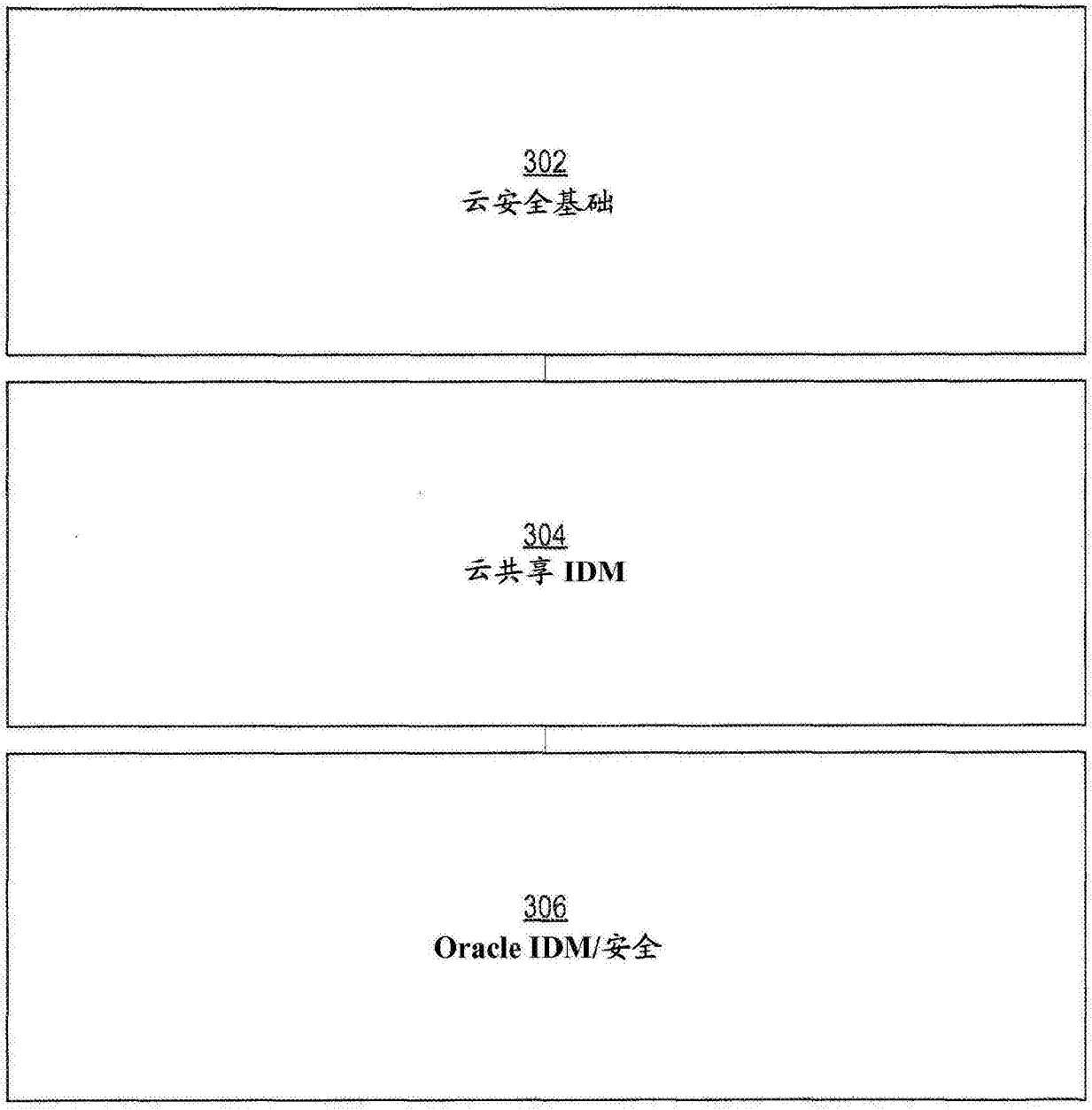


图3

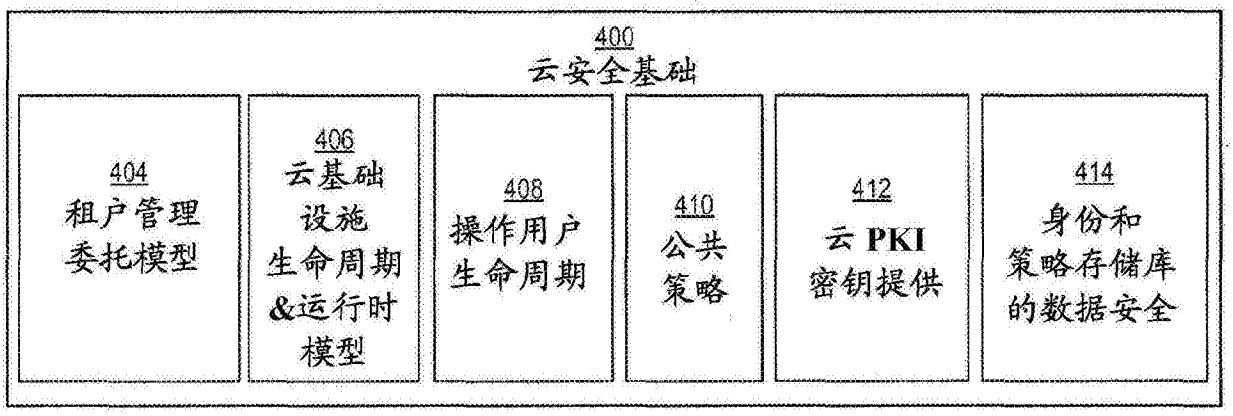

400
云安全基础
404
租户管理
委托模型
406
云基础
设施
生命周期
&运行时
模型
408
操作用户
生命周期
410
公共
策略
412
云 PKI
密钥提供
414
身份和
策略存储库
的数据安全

图4

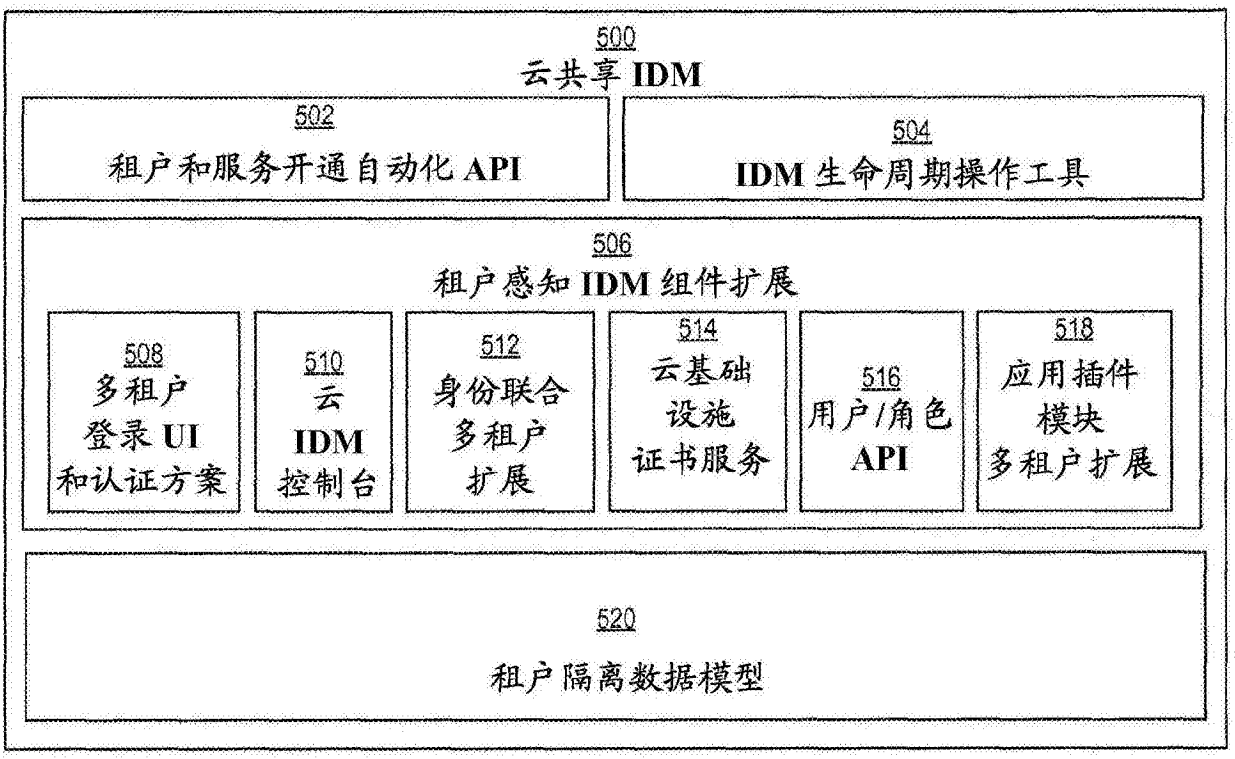

500
云共享 IDM
502
租户和服务开通自动化 API
504
IDM 生命周期操作工具
506
租户感知 IDM 组件扩展
508
多租户
登录 UI
和认证方案
510
云
IDM
控制台
512
身份联合
多租户
扩展
514
云基础
设施
证书服务
516
用户/角色
API
518
应用插件
模块
多租户扩展
520
租户隔离数据模型

图5

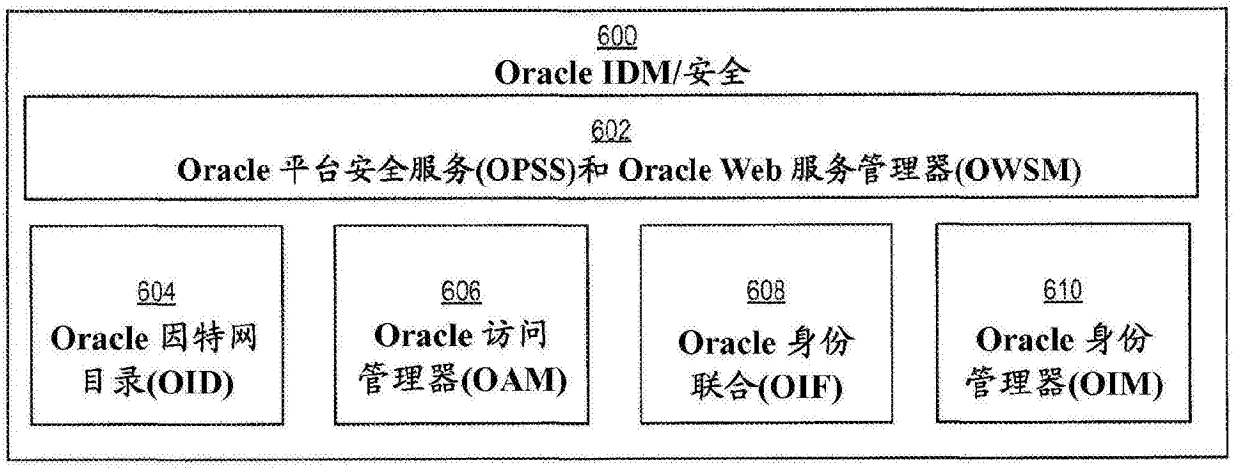

600
Oracle IDM/安全
602
Oracle 平台安全服务(OPSS)和 Oracle Web 服务管理器(OWSM)
604
Oracle 因特网目录(OID)
606
Oracle 访问管理器(OAM)
608
Oracle 身份联合(OIF)
610
Oracle 身份管理器(OIM)

图6

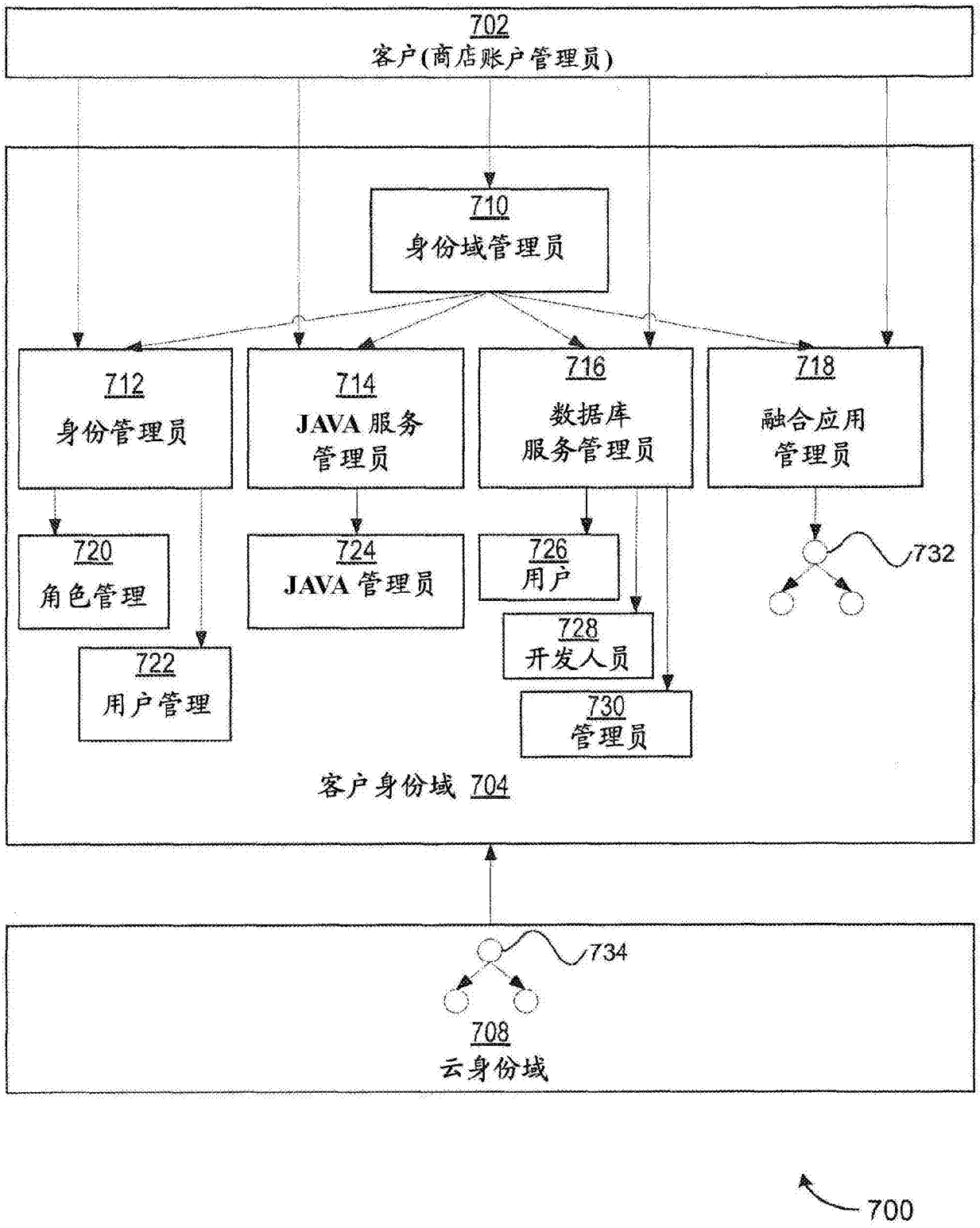

702
客户(商店账户管理员)
710
身份域管理员
712
身份管理员
714
JAVA 服务
管理员
716
数据库
服务管理员
718
融合应用
管理员
720
角色管理
722
用户管理
724
JAVA 管理员
726
用户
728
开发人员
730
管理员
732
客户身份域 704
734
708
云身份域
700

图7

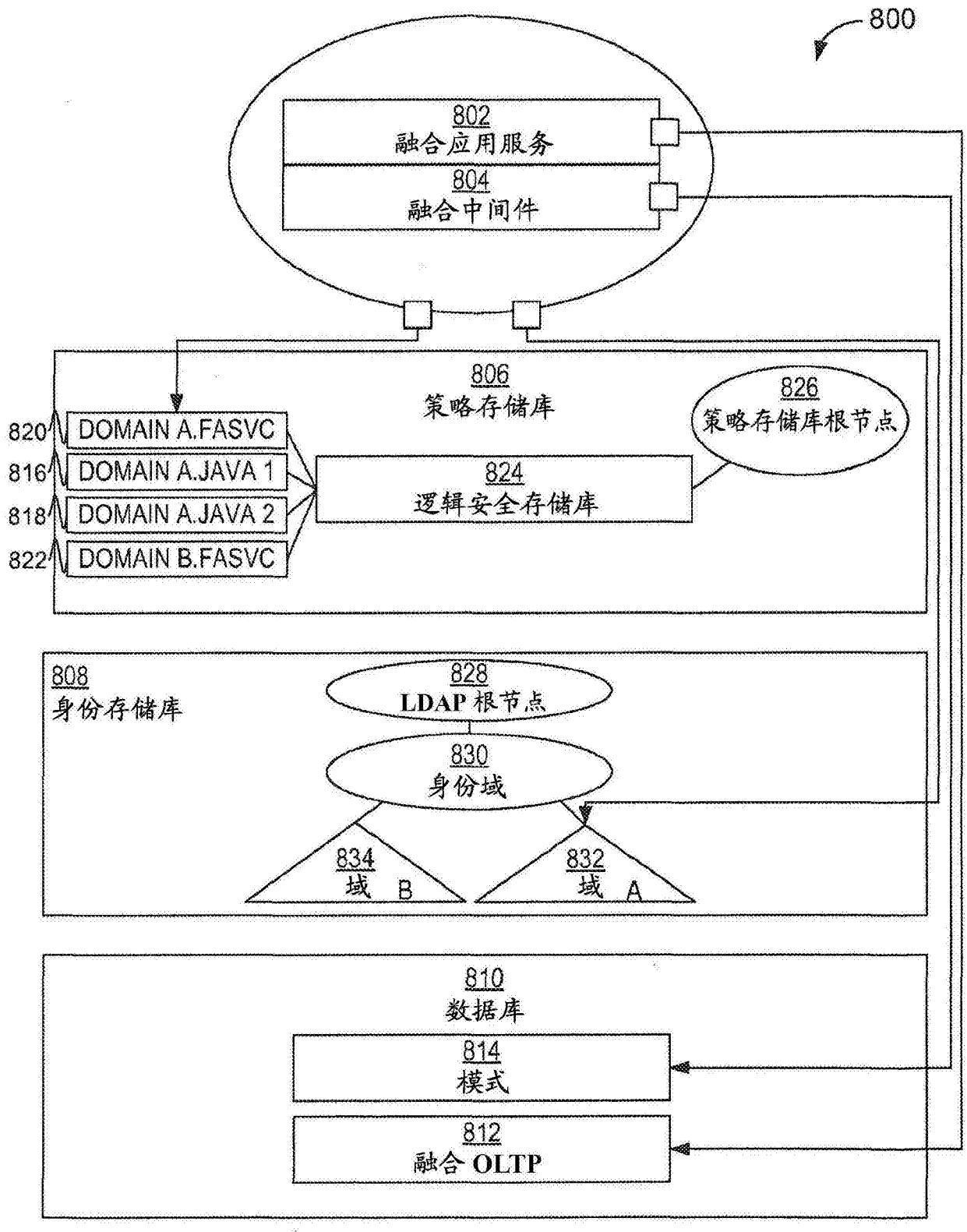

800
802
融合应用服务
804
融合中间件
806
策略存储库
826
策略存储库根节点
820
DOMAIN A.FASVC
816
DOMAIN A.JAVA 1
818
DOMAIN A.JAVA 2
822
DOMAIN B.FASVC
824
逻辑安全存储库
808
身份存储库
828
LDAP 根节点
830
身份域
834
域 B
832
域 A
810
数据库
814
模式
812
融合 OLTP

图8

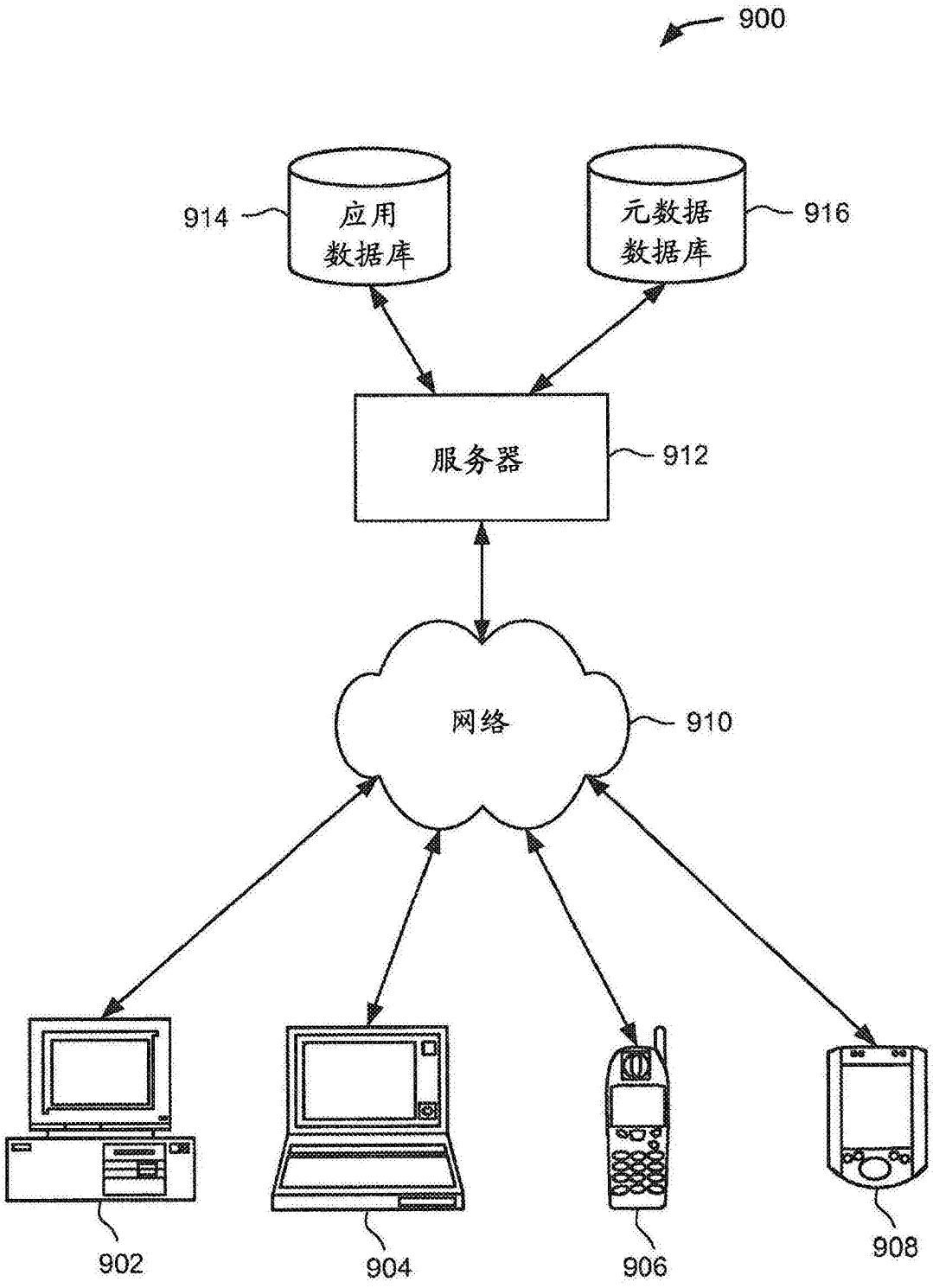


图9

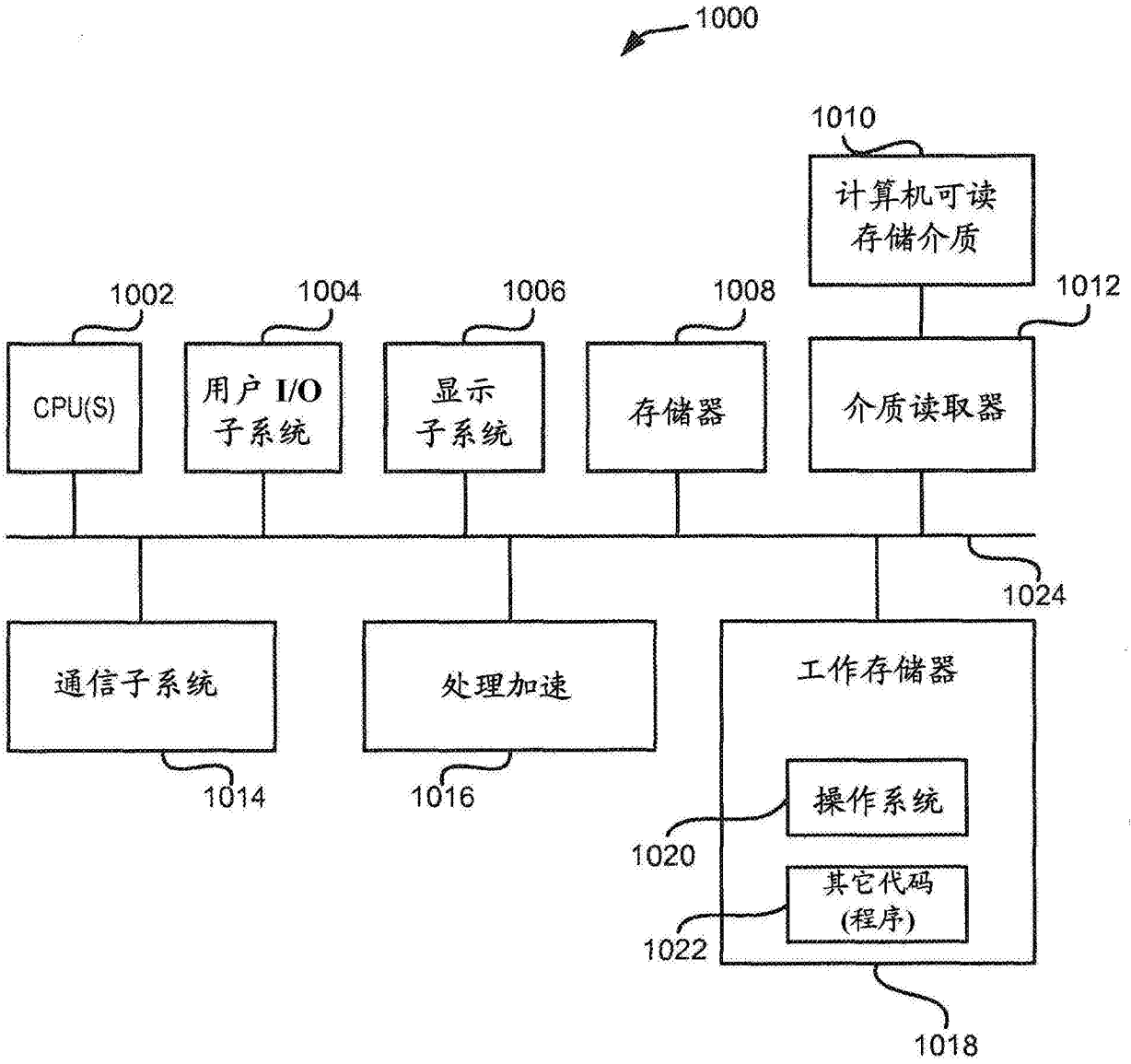

1000
1010
计算机可读
存储介质
1002
1004
1006
1008
1012
CPU(S)
用户 I/O
子系统
显示
子系统
存储器
介质读取器
1024
通信子系统
处理加速
工作存储器
1014
1016
操作系统
1020
其它代码
(程序)
1022
1018

图10

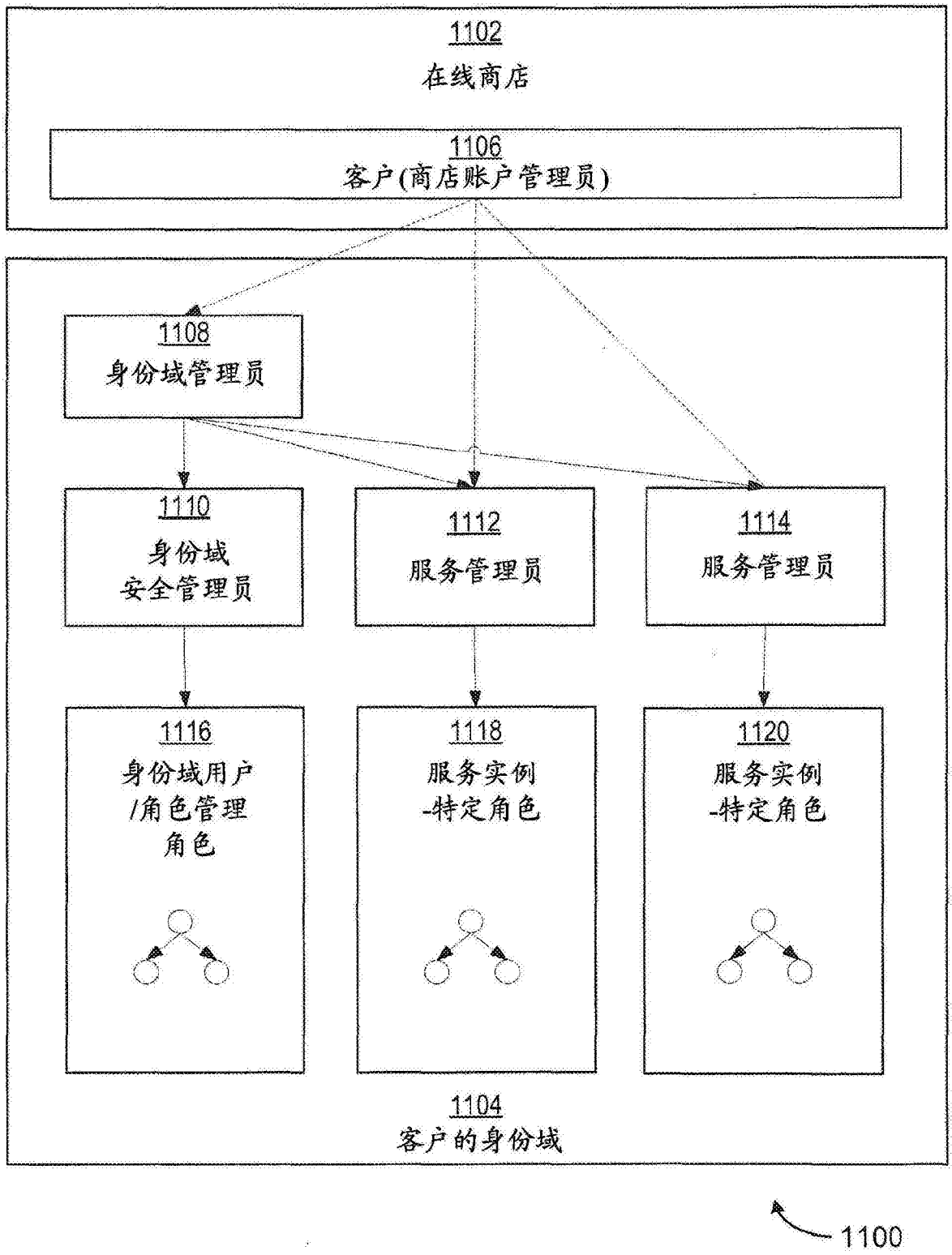

1102
在线商店
1106
客户(商店账户管理员)
1108
身份域管理员
1110
身份域
安全管理员
1112
服务管理员
1114
服务管理员
1116
身份域用户
/角色管理
角色
1118
服务实例
-特定角色
1120
服务实例
-特定角色
1104
客户的身份域
1100

图11

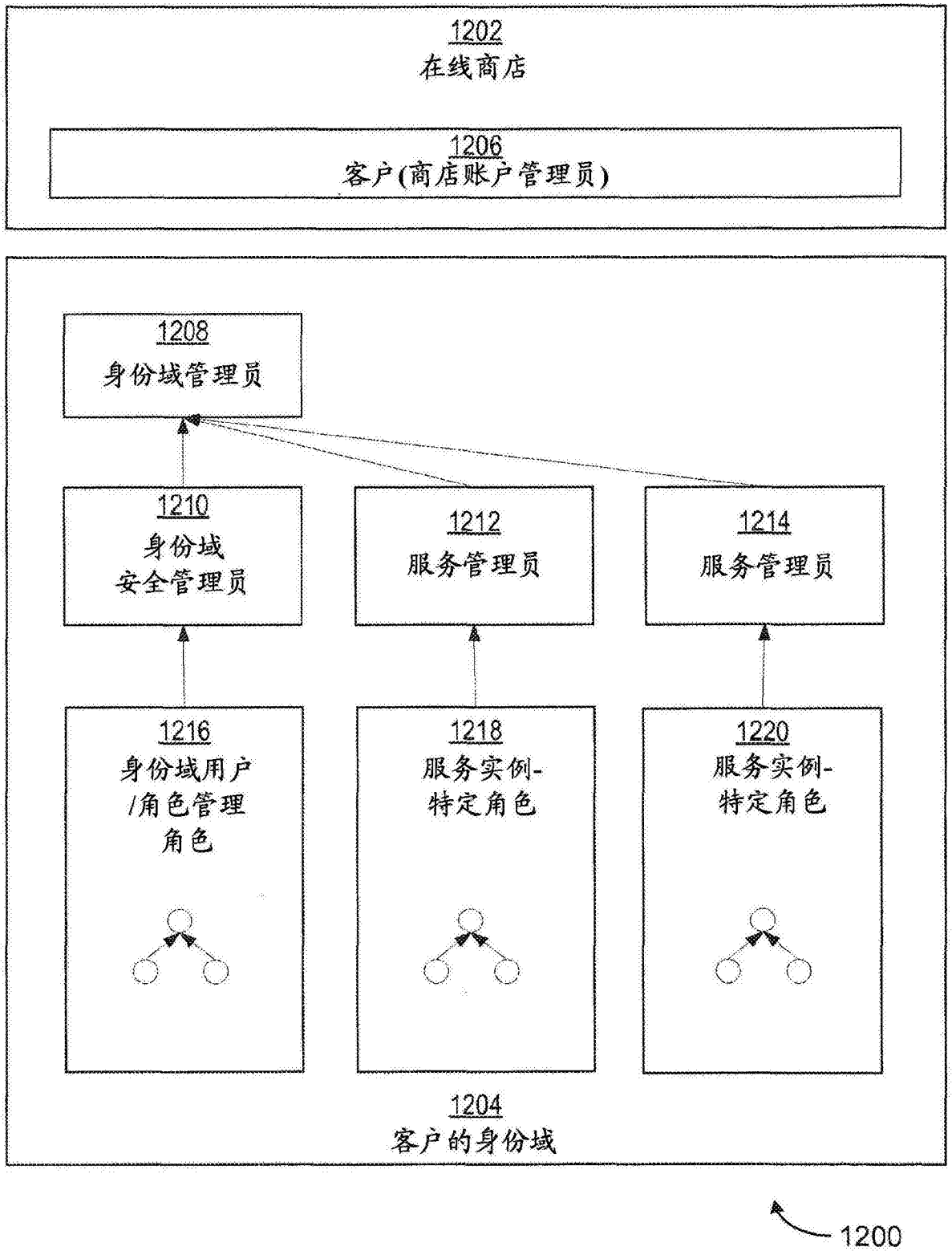

1202
在线商店
1206
客户(商店账户管理员)
1208
身份域管理员
1210
身份域
安全管理员
1212
服务管理员
1214
服务管理员
1216
身份域用户
/角色管理
角色
1218
服务实例-
特定角色
1220
服务实例-
特定角色
1204
客户的身份域
1200

图12

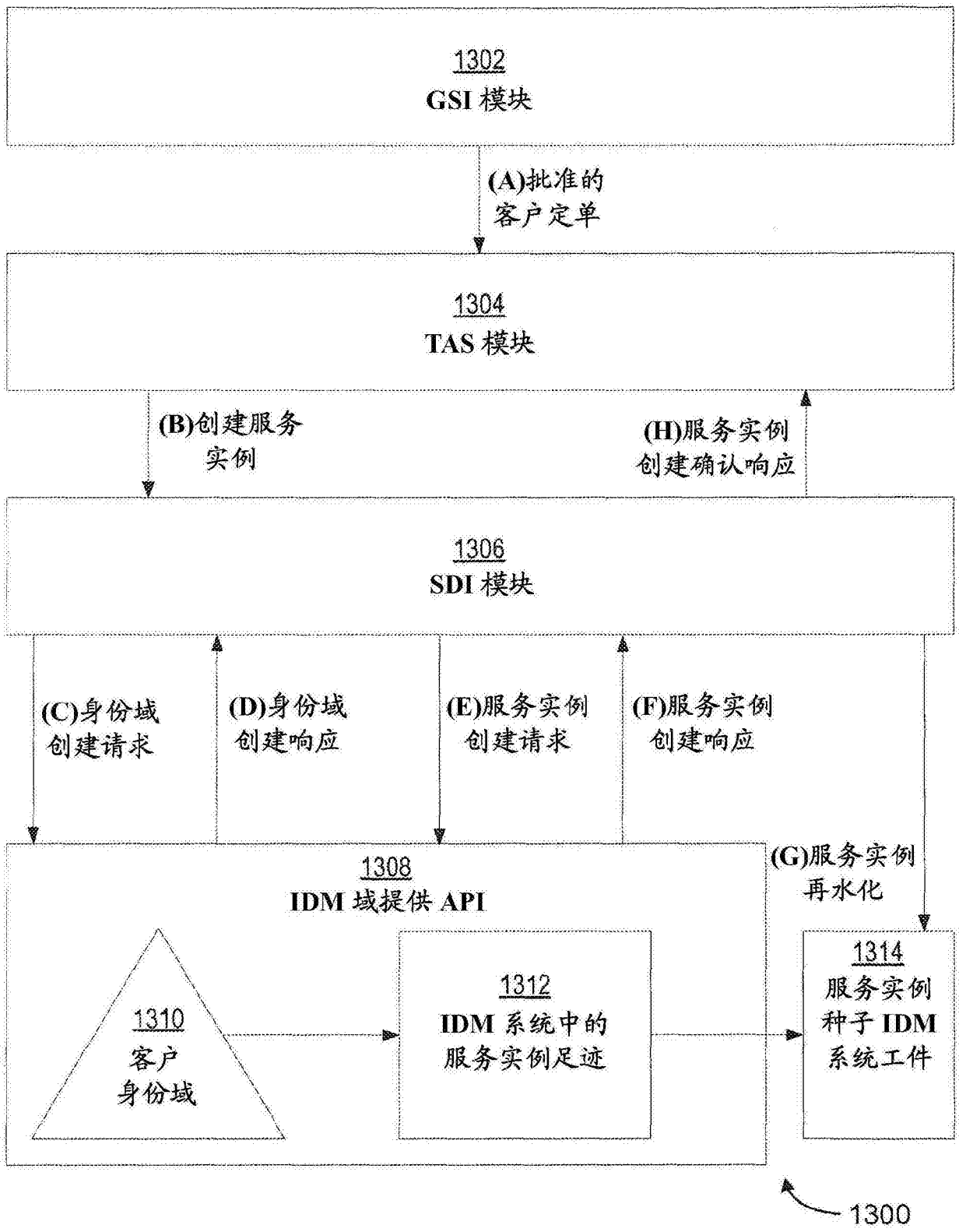

1302
GSI 模块
(A)批准的
客户定单
1304
TAS 模块
(B)创建服务
实例
(H)服务实例
创建确认响应
1306
SDI 模块
(C)身份域
创建请求
(D)身份域
创建响应
(E)服务实例
创建请求
(F)服务实例
创建响应
(G)服务实例
再水化
1308
IDM 域提供 API
1310
客户
身份域
1312
IDM 系统中的
服务实例足迹
1314
服务实例
种子 IDM
系统工件
1300

图13

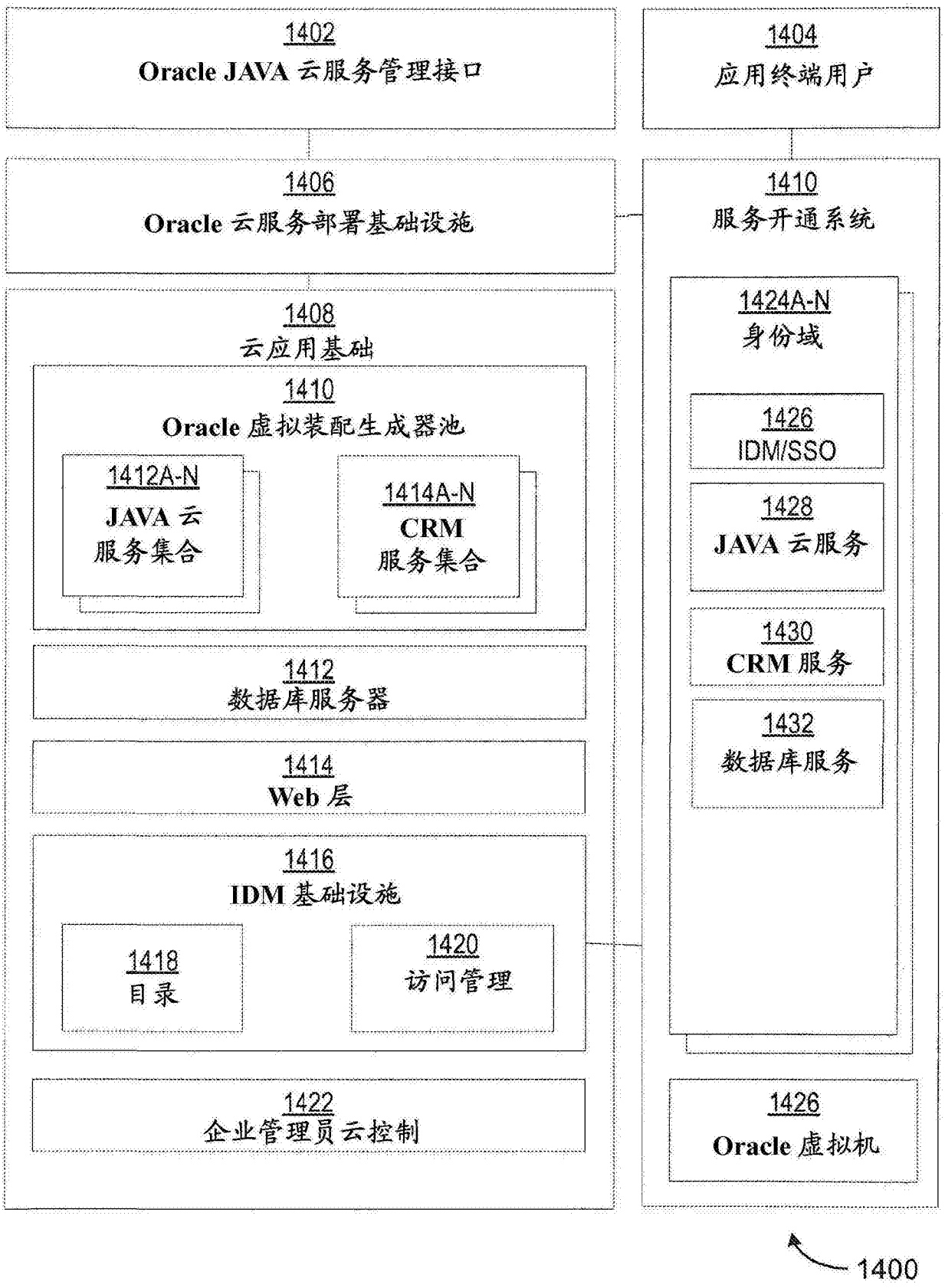

1402
Oracle JAVA 云服务管理接口
1404
应用终端用户
1406
Oracle 云服务部署基础设施
1410
服务开通系统
1408
云应用基础
1424A-N
身份域
1410
Oracle 虚拟装配生成器池
1426
IDM/SSO
1412A-N
JAVA 云
服务集合
1414A-N
CRM
服务集合
1428
JAVA 云服务
1430
CRM 服务
1412
数据库服务器
1432
数据库服务
1414
Web 层
1416
IDM 基础设施
1418
目录
1420
访问管理
1422
企业管理员云控制
1426
Oracle 虚拟机
1400

图14

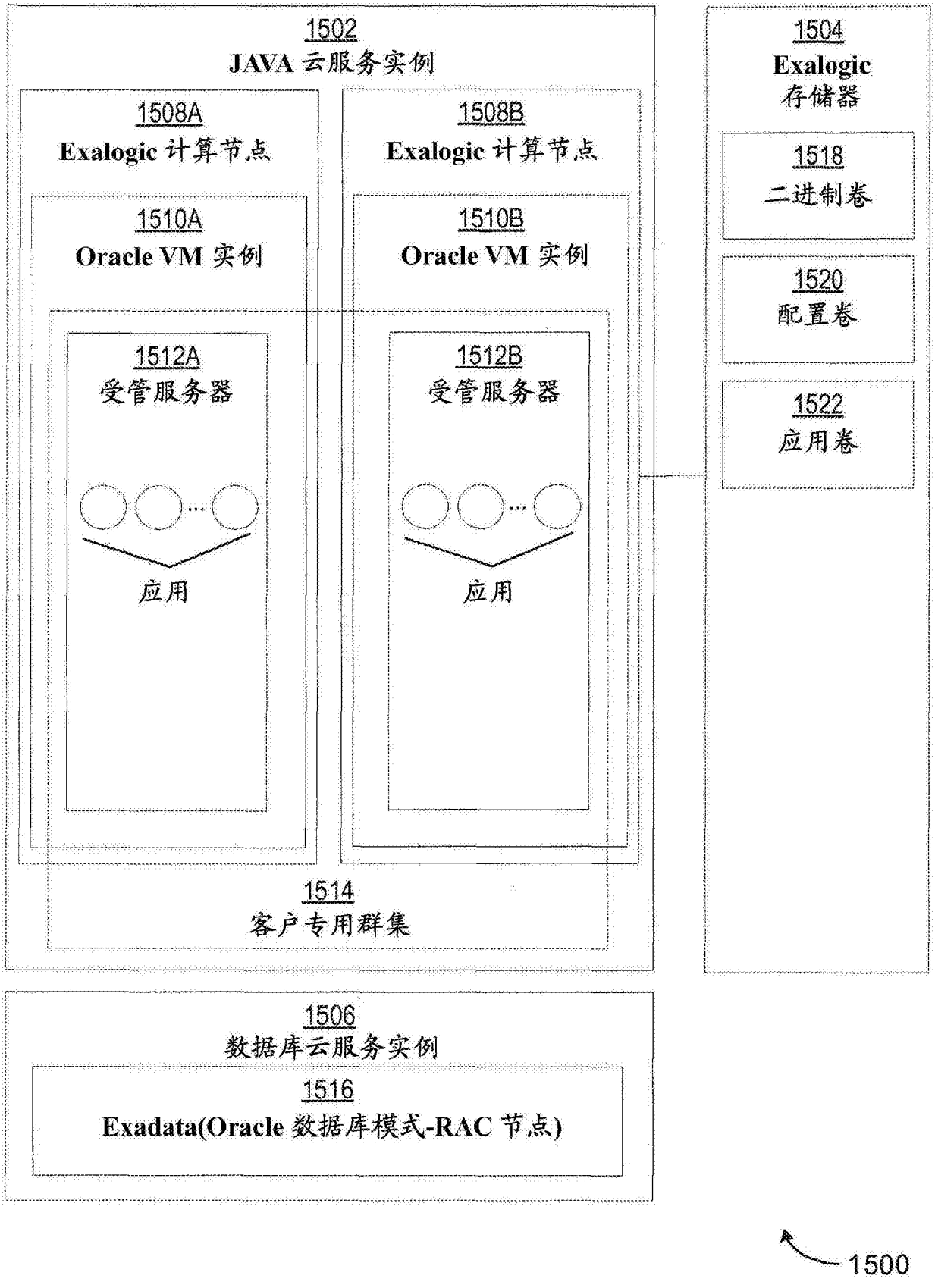

1502
JAVA 云服务实例
1508A
Exalogic 计算节点
1508B
Exalogic 计算节点
1510A
Oracle VM 实例
1510B
Oracle VM 实例
1512A
受管服务器
1512B
受管服务器
应用
应用
1514
客户专用群集
1504
Exalogic
存储器
1518
二进制卷
1520
配置卷
1522
应用卷
1506
数据库云服务实例
1516
Exadata(Oracle 数据库模式-RAC 节点)
1500

图15

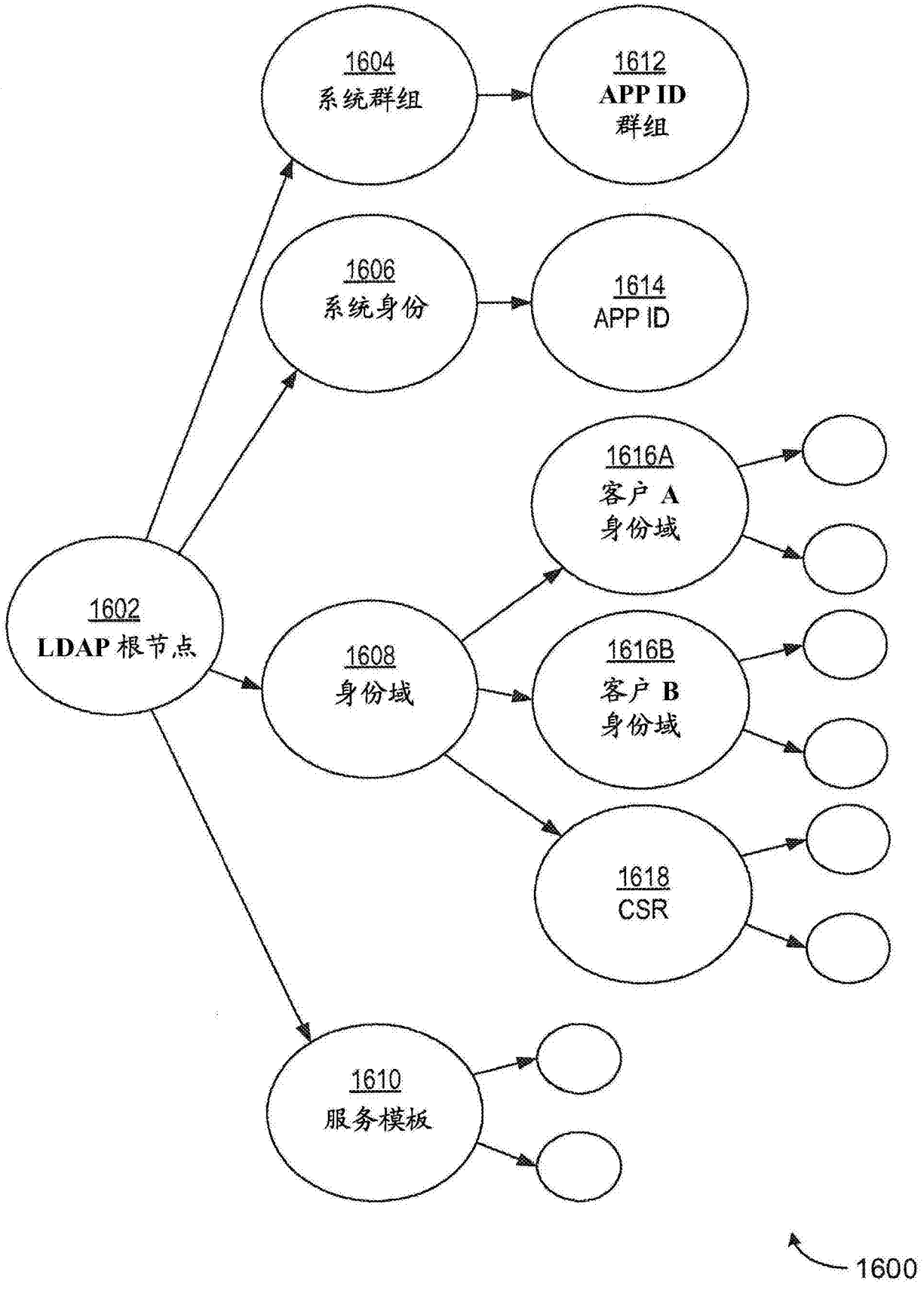

1604
系统群组
1612
APP ID
群组
1606
系统身份
1614
APP ID
1616A
客户 A
身份域
1602
LDAP 根节点
1608
身份域
1616B
客户 B
身份域
1618
CSR
1610
服务模板
1600

图16

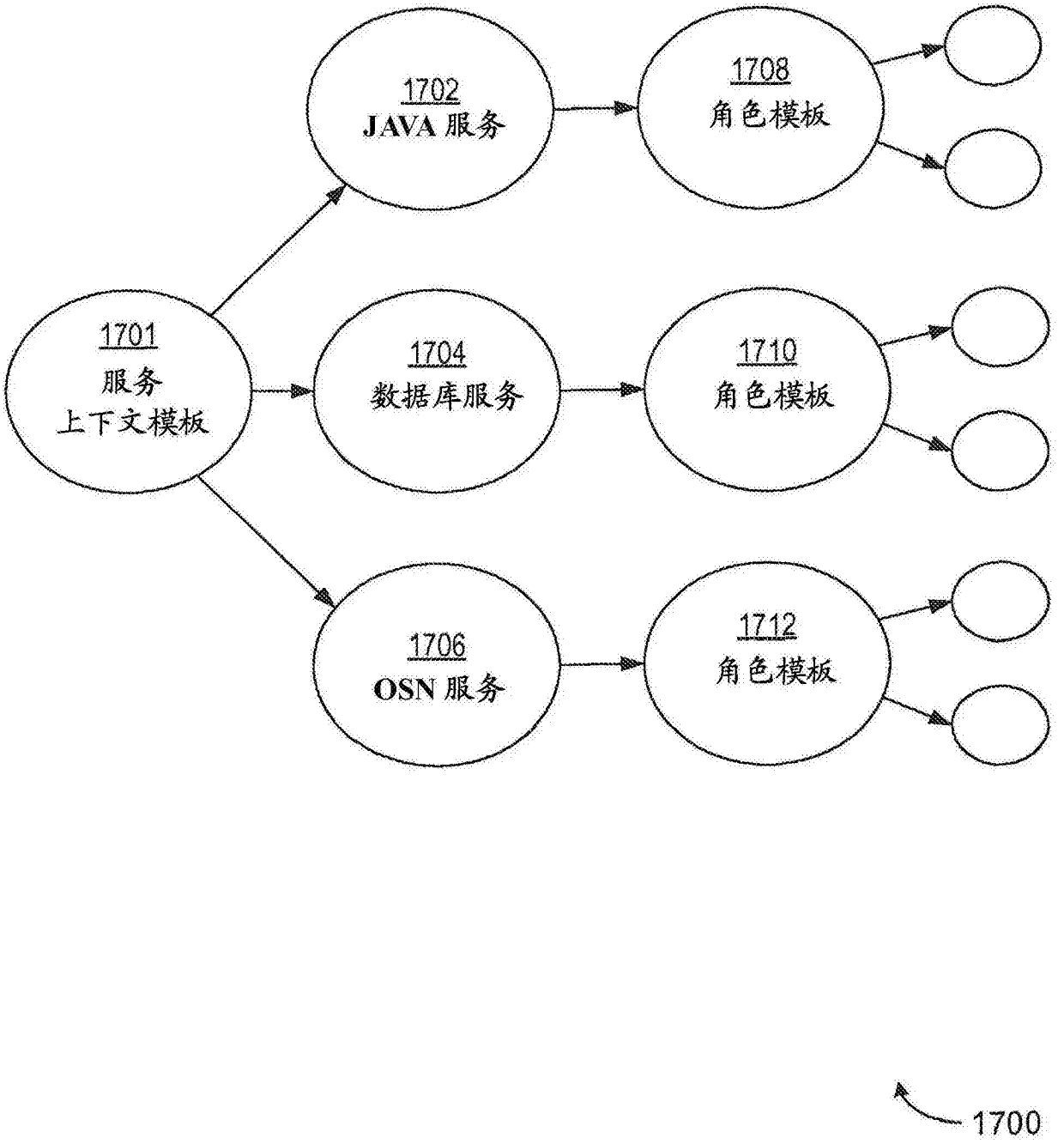

1702
JAVA 服务
1708
角色模板
1701
服务
上下文模板
1704
数据库服务
1710
角色模板
1706
OSN 服务
1712
角色模板
1700

图17

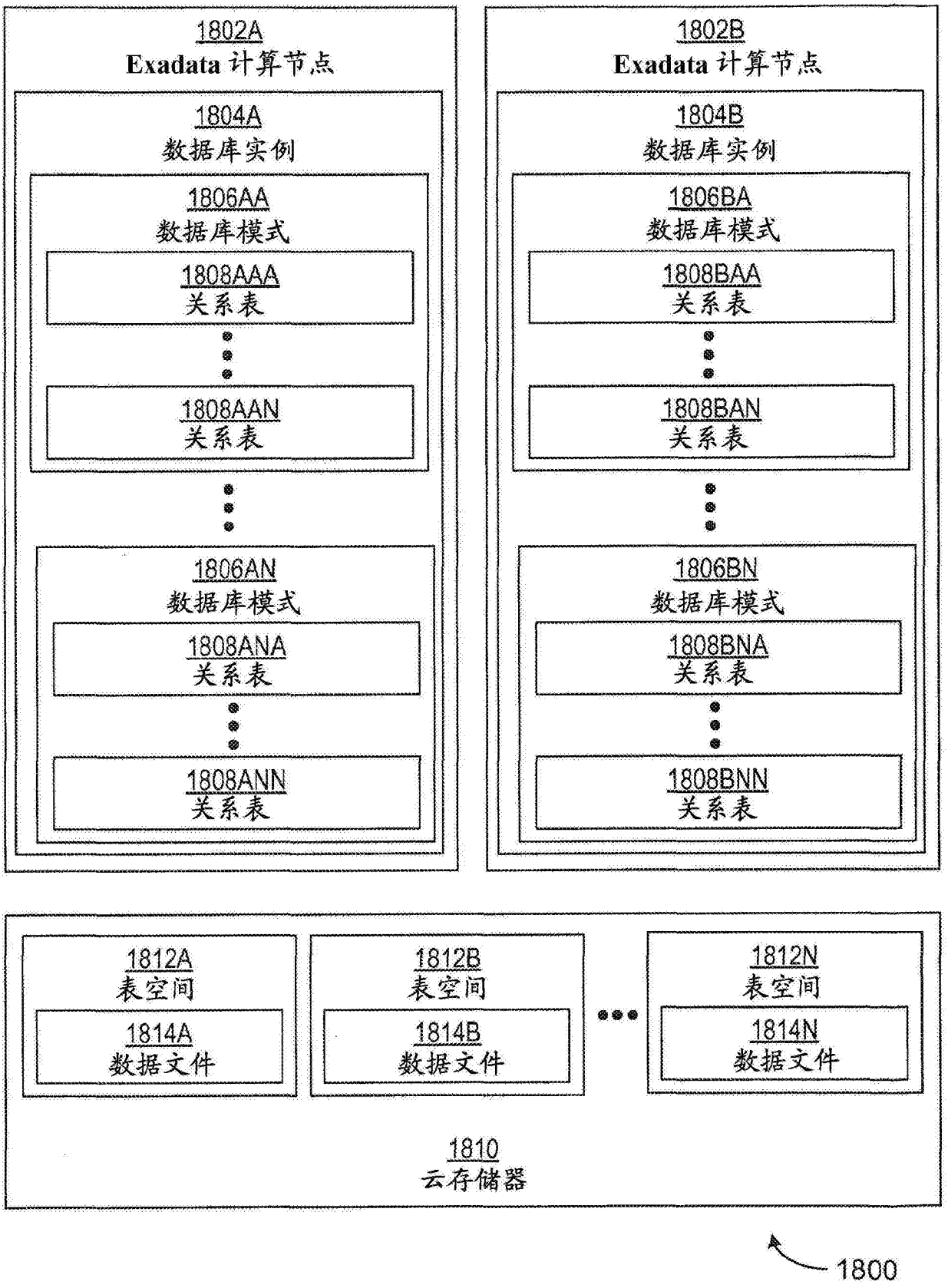

1802A
Exadata 计算节点
1804A
数据库实例
1806AA
数据库模式
1808AAA
关系表
1808AAN
关系表
1806AN
数据库模式
1808ANA
关系表
1808ANN
关系表
1802B
Exadata 计算节点
1804B
数据库实例
1806BA
数据库模式
1808BAA
关系表
1808BAN
关系表
1806BN
数据库模式
1808BNA
关系表
1808BNN
关系表
1812A
表空间
1814A
数据文件
1812B
表空间
1814B
数据文件
1812N
表空间
1814N
数据文件
1810
云存储器
1800

图18

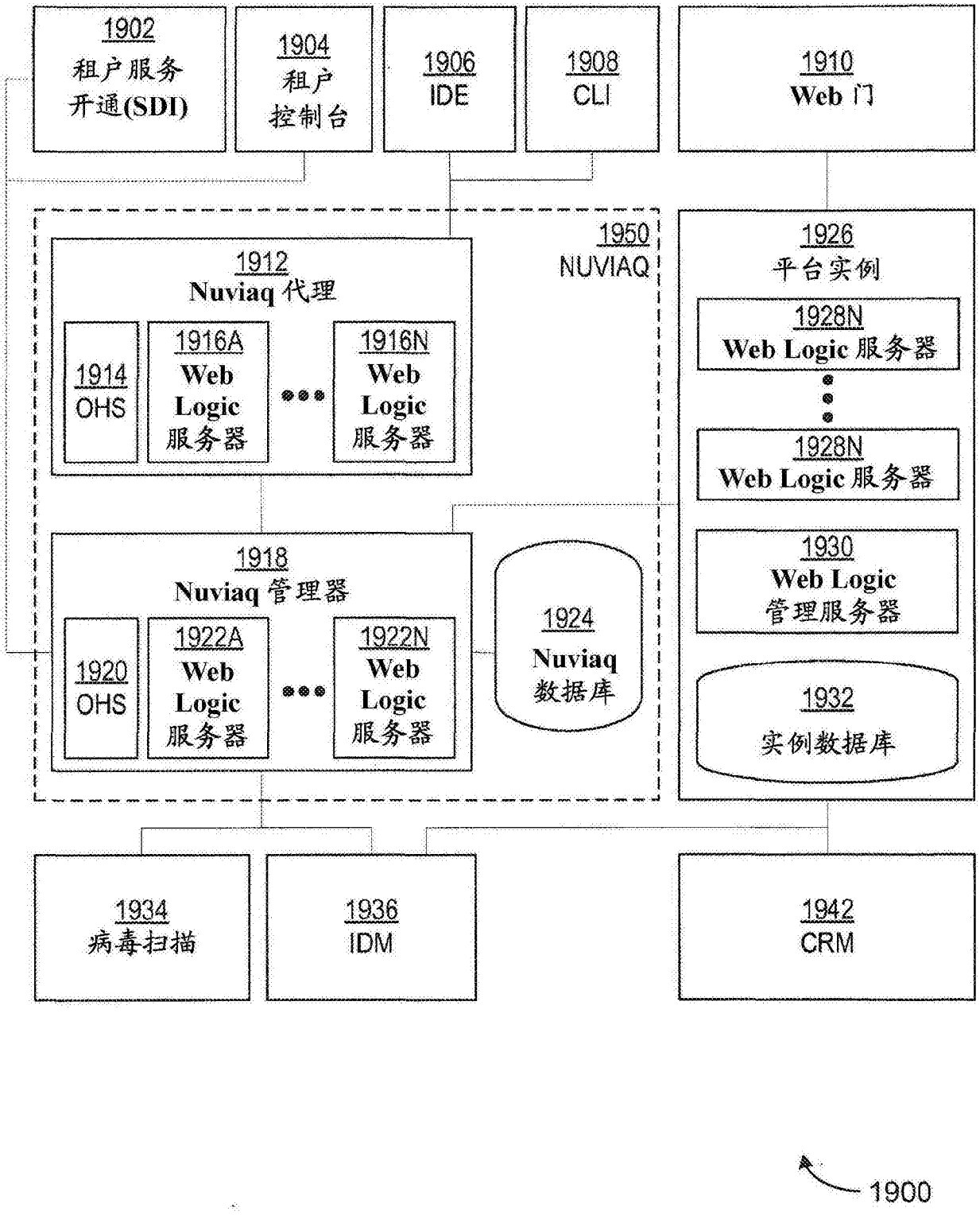

1902
租户服务
开通(SDI)
1904
租户
控制台
1906
IDE
1908
CLI
1910
Web 门
1950
NUVIAQ
1912
Nuviaq 代理
1914
OHS
1916A
Web
Logic
服务器
1916N
Web
Logic
服务器
1918
Nuviaq 管理器
1920
OHS
1922A
Web
Logic
服务器
1922N
Web
Logic
服务器
1924
Nuviaq
数据库
1926
平台实例
1928N
Web Logic 服务器
1928N
Web Logic 服务器
1930
Web Logic
管理服务器
1932
实例数据库
1934
病毒扫描
1936
IDM
1942
CRM
1900

图19

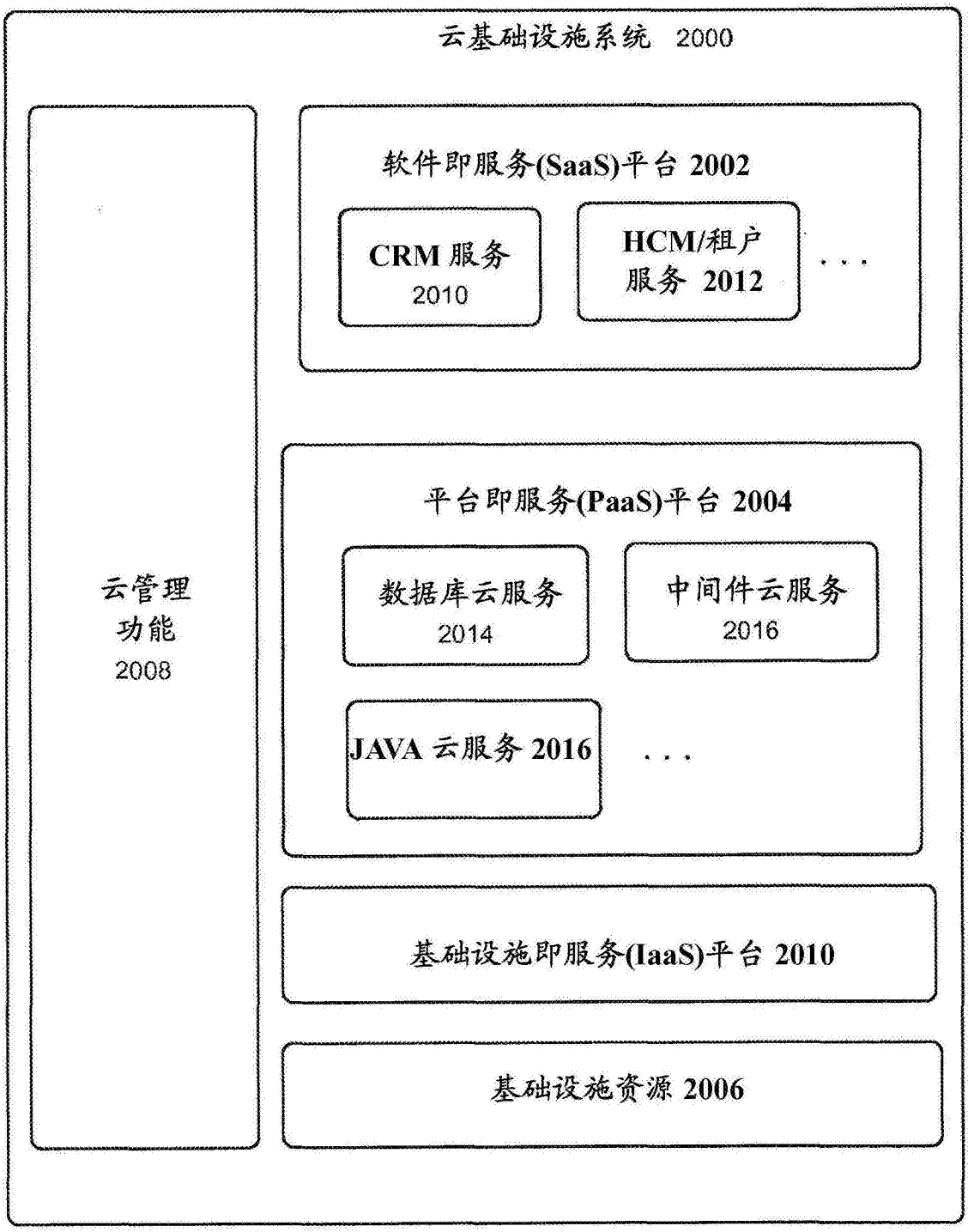

云基础设施系统 2000
软件即服务(SaaS)平台 2002
CRM 服务 2010
HCM/租户服务 2012
. . .
平台即服务(PaaS)平台 2004
数据库云服务 2014
中间件云服务 2016
JAVA 云服务 2016
. . .
基础设施即服务(IaaS)平台 2010
基础设施资源 2006
云管理功能 2008

图20A

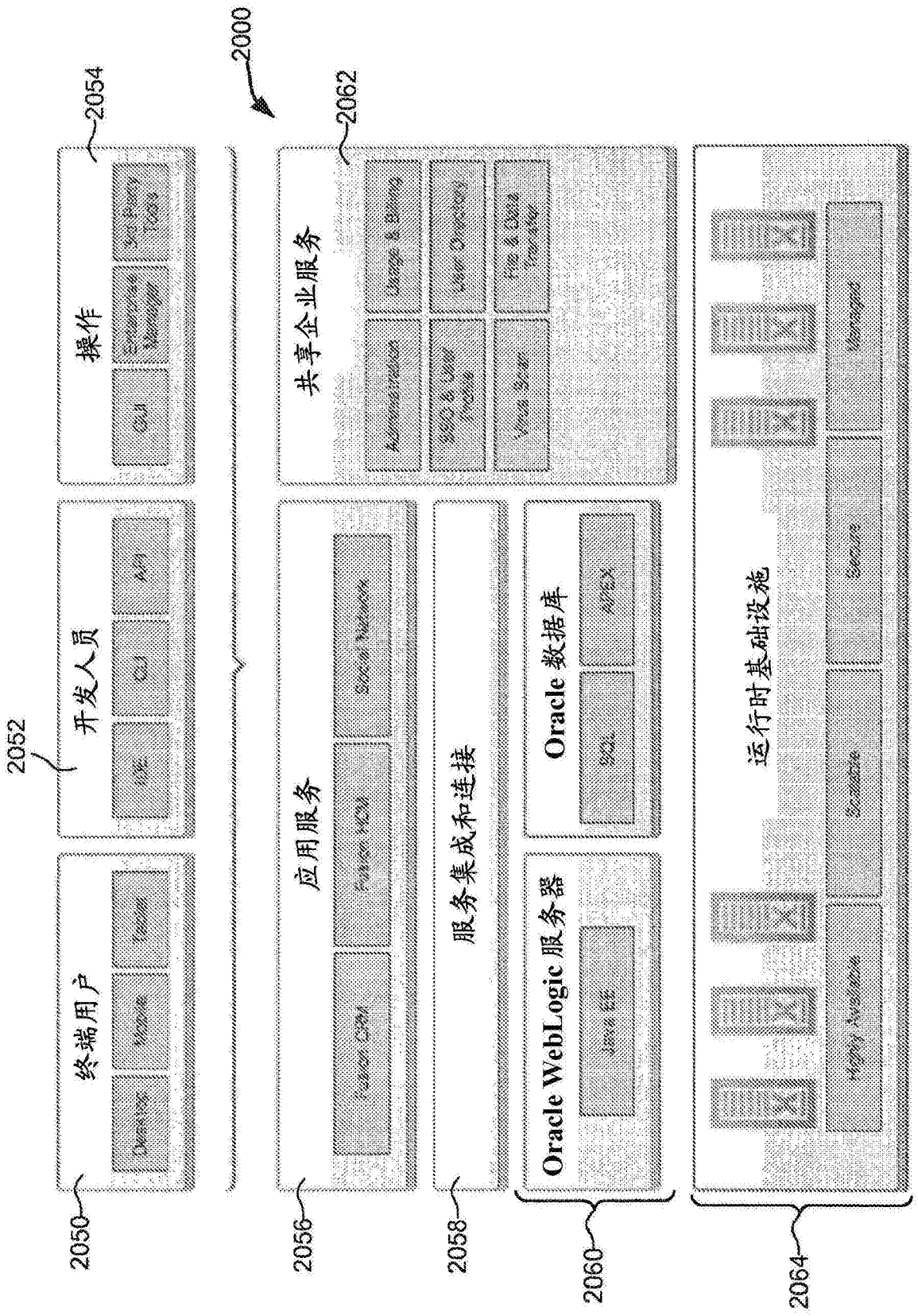

2000
2050
终端用户
2052
开发人员
2054
操作
2056
应用服务
2058
服务集成和连接
2060
Oracle WebLogic 服务器
Oracle 数据库
2062
共享企业服务
2064
运行时基础设施

图20B

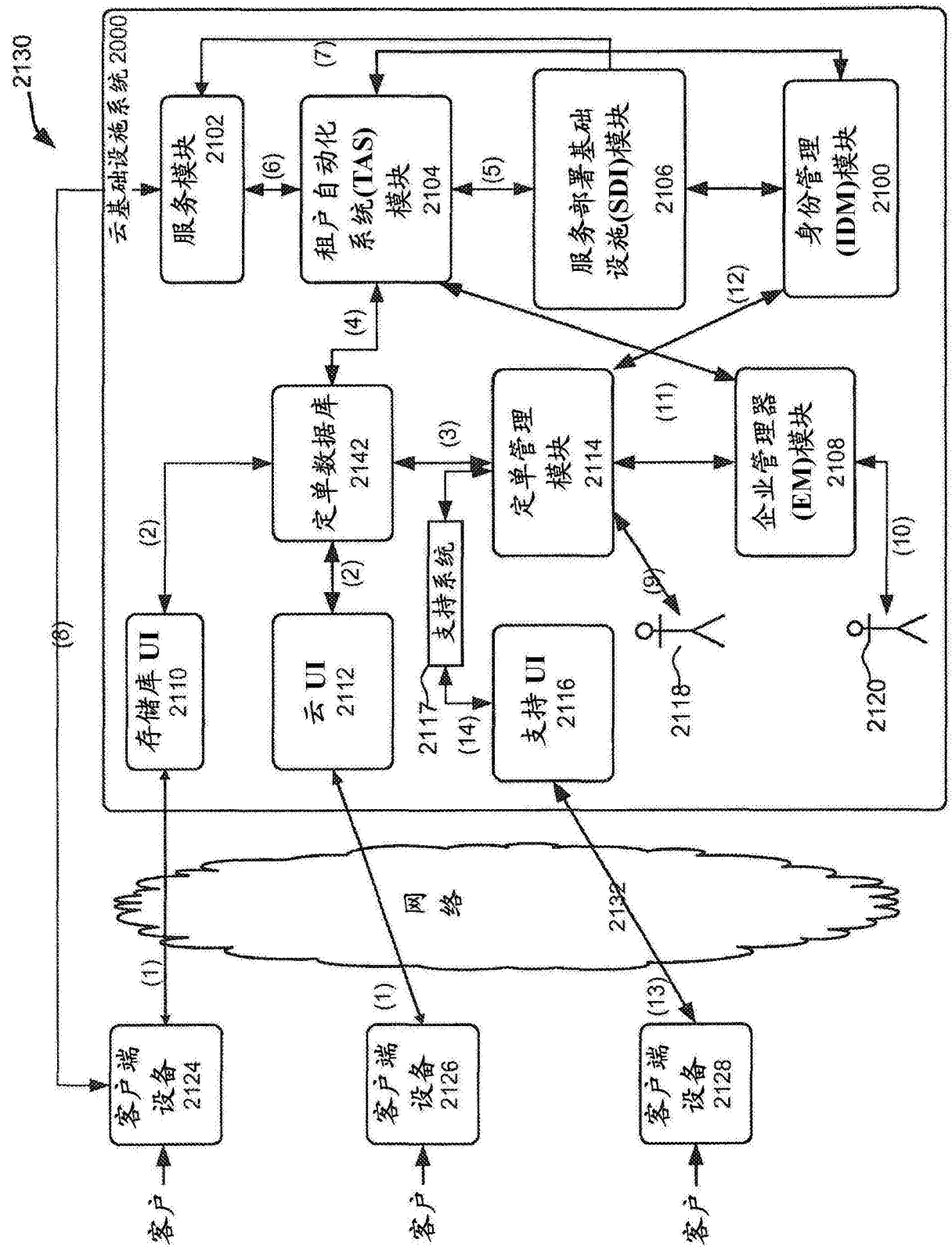

2130
云基础设施系统2000
服务模块 2102
租户自动化系统(TAS)模块 2104
服务部署基础设施(SDI)模块 2106
身份管理(IDM)模块 2100
定单数据库 2142
定单管理模块 2114
企业管理器(EM)模块 2108
存储库 UI 2110
云 UI 2112
支持系统
支持 UI 2116
2117
2118
2120
网络
2132
客户端设备 2124
客户端设备 2126
客户端设备 2128
客户
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14)

图21

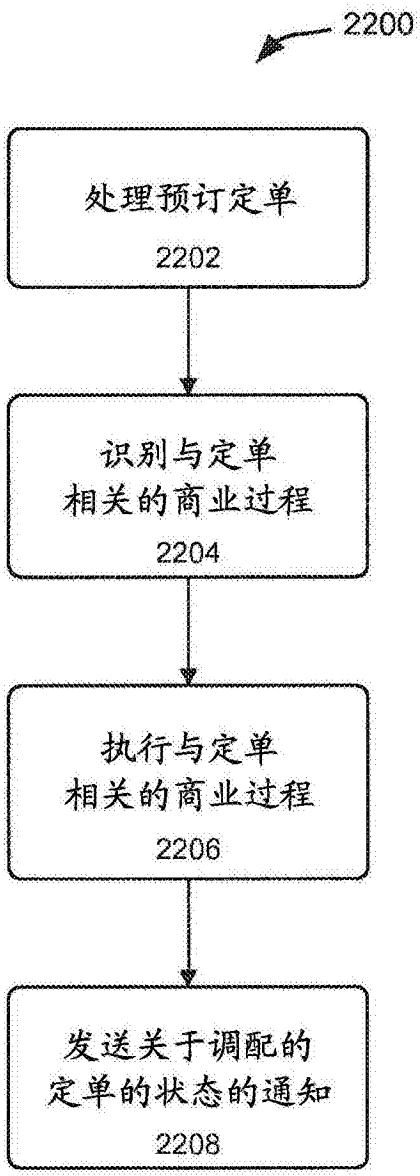

2200
处理预订定单
2202
识别与定单
相关的商业过程
2204
执行与定单
相关的商业过程
2206
发送关于调配的
定单的状态的通知
2208

图22A

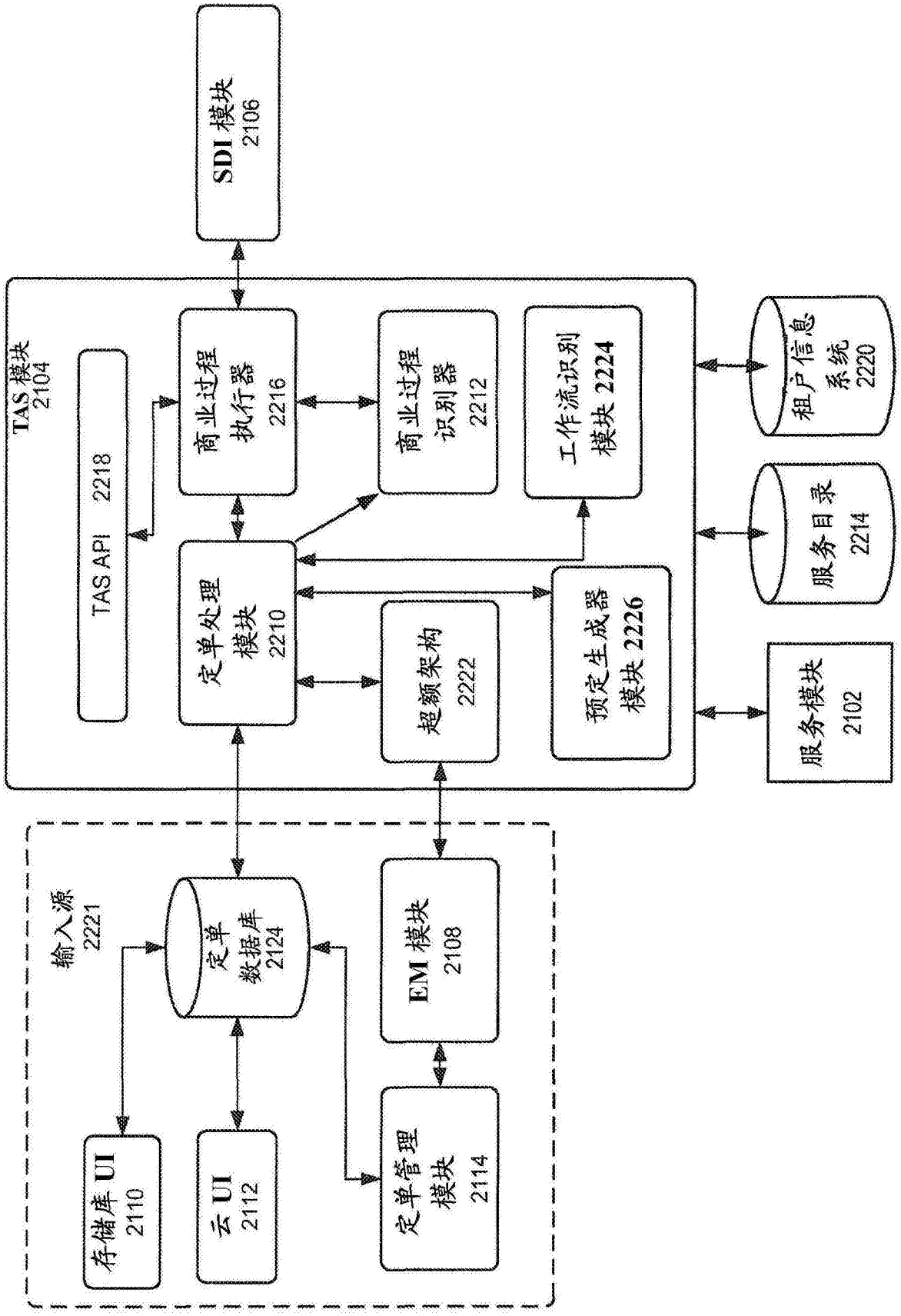

SDI 模块
2106
TAS 模块
2104
TAS API 2218
商业过程
执行器
2216
商业过程
识别器
2212
工作流识别
模块 2224
租户信息
系统
2220
定单处理
模块
2210
超额架构
2222
预定生成器
模块 2226
服务目录
2214
服务模块
2102
输入源
2221
定单
数据库
2124
EM 模块
2108
存储库 UI
2110
云 UI
2112
定单管理
模块
2114

图22B

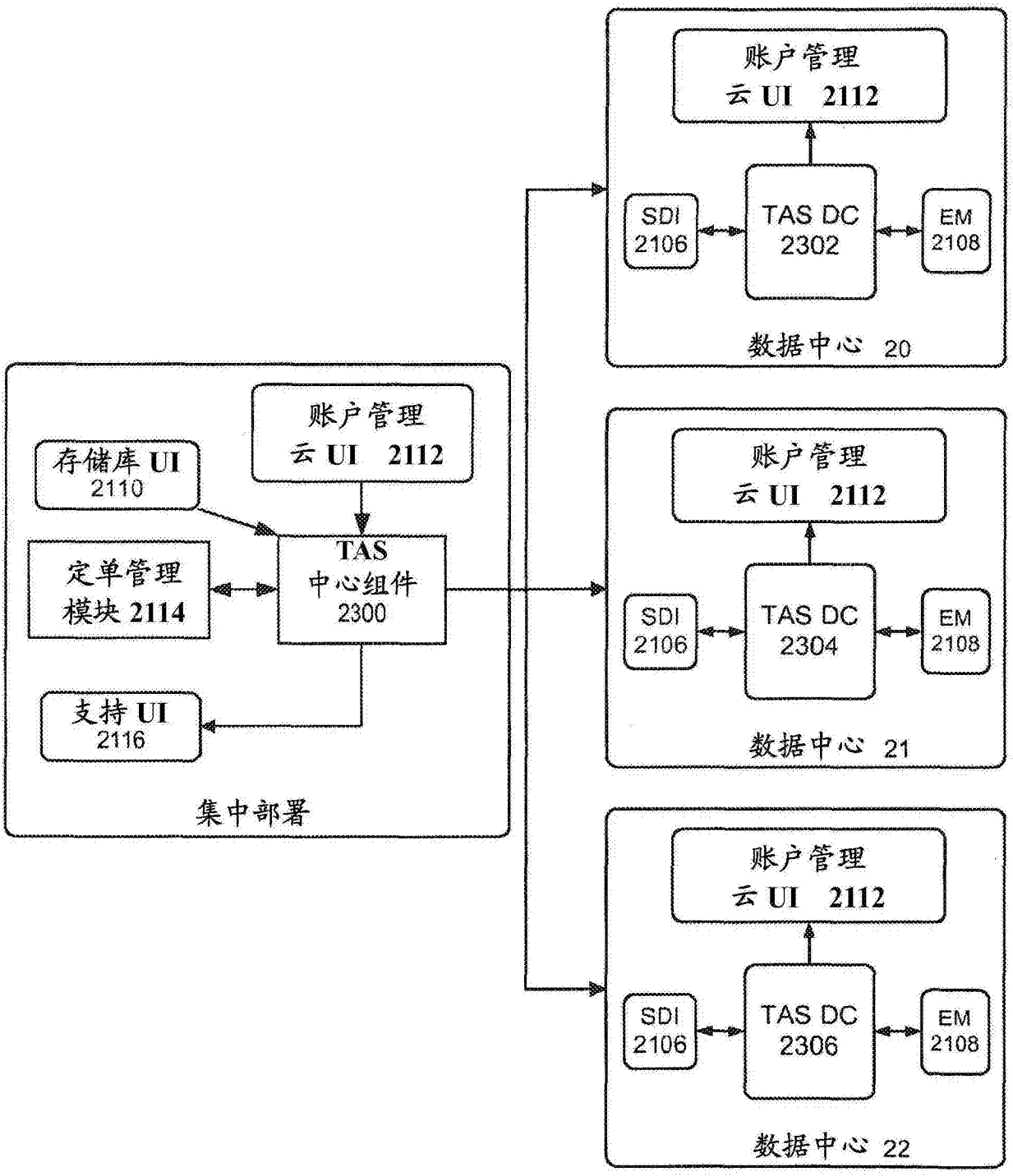

账户管理
云 UI 2112
SDI
2106
TAS DC
2302
EM
2108
数据中心 20
账户管理
云 UI 2112
存储库 UI
2110
TAS
中心组件
2300
定单管理
模块 2114
支持 UI
2116
集中部署
账户管理
云 UI 2112
SDI
2106
TAS DC
2304
EM
2108
数据中心 21
账户管理
云 UI 2112
SDI
2106
TAS DC
2306
EM
2108
数据中心 22

图23

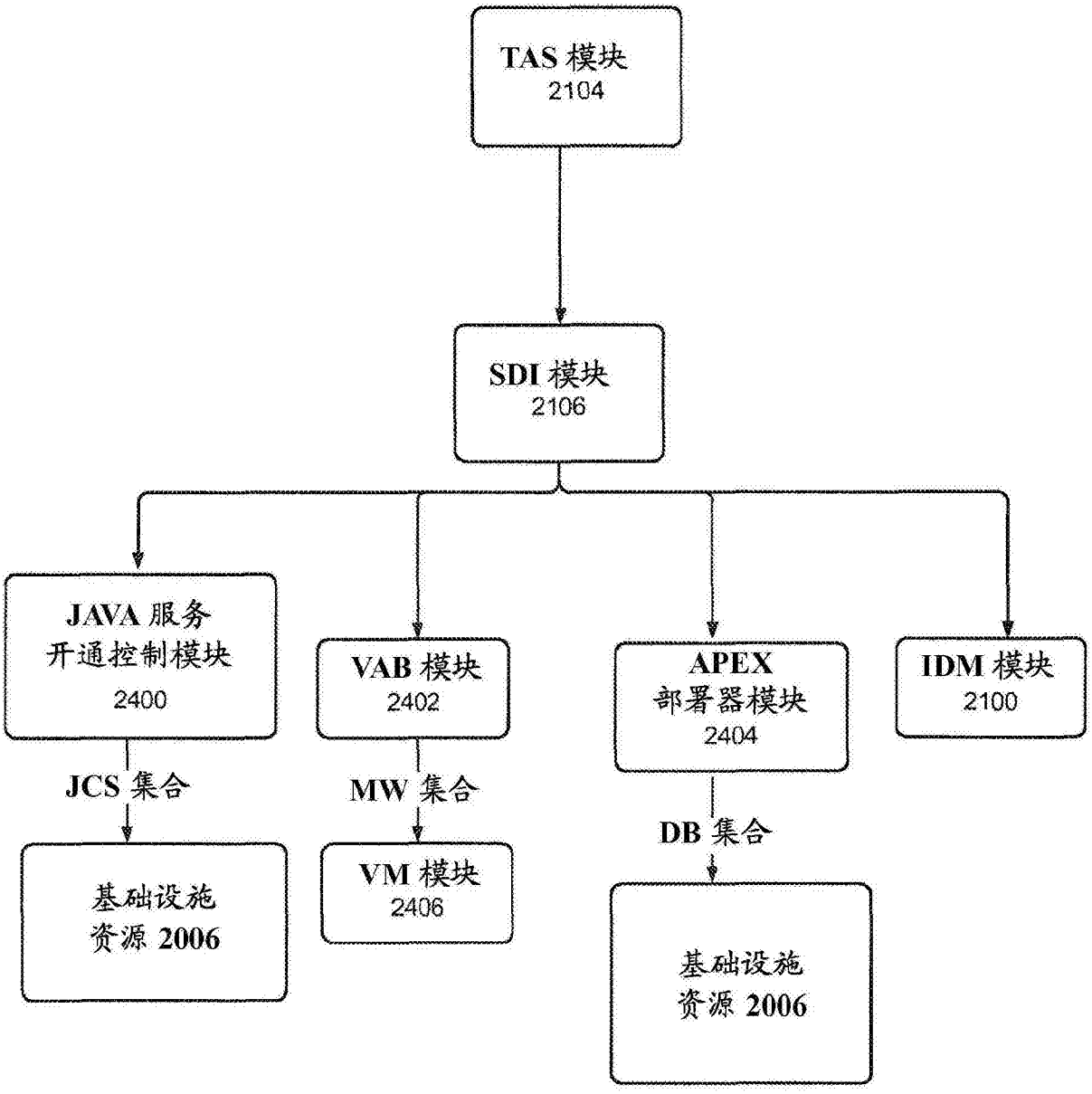

TAS 模块
2104
SDI 模块
2106
JAVA 服务
开通控制模块
2400
VAB 模块
2402
APEX
部署器模块
2404
IDM 模块
2100
JCS 集合
MW 集合
DB 集合
基础设施
资源 2006
VM 模块
2406
基础设施
资源 2006

图24

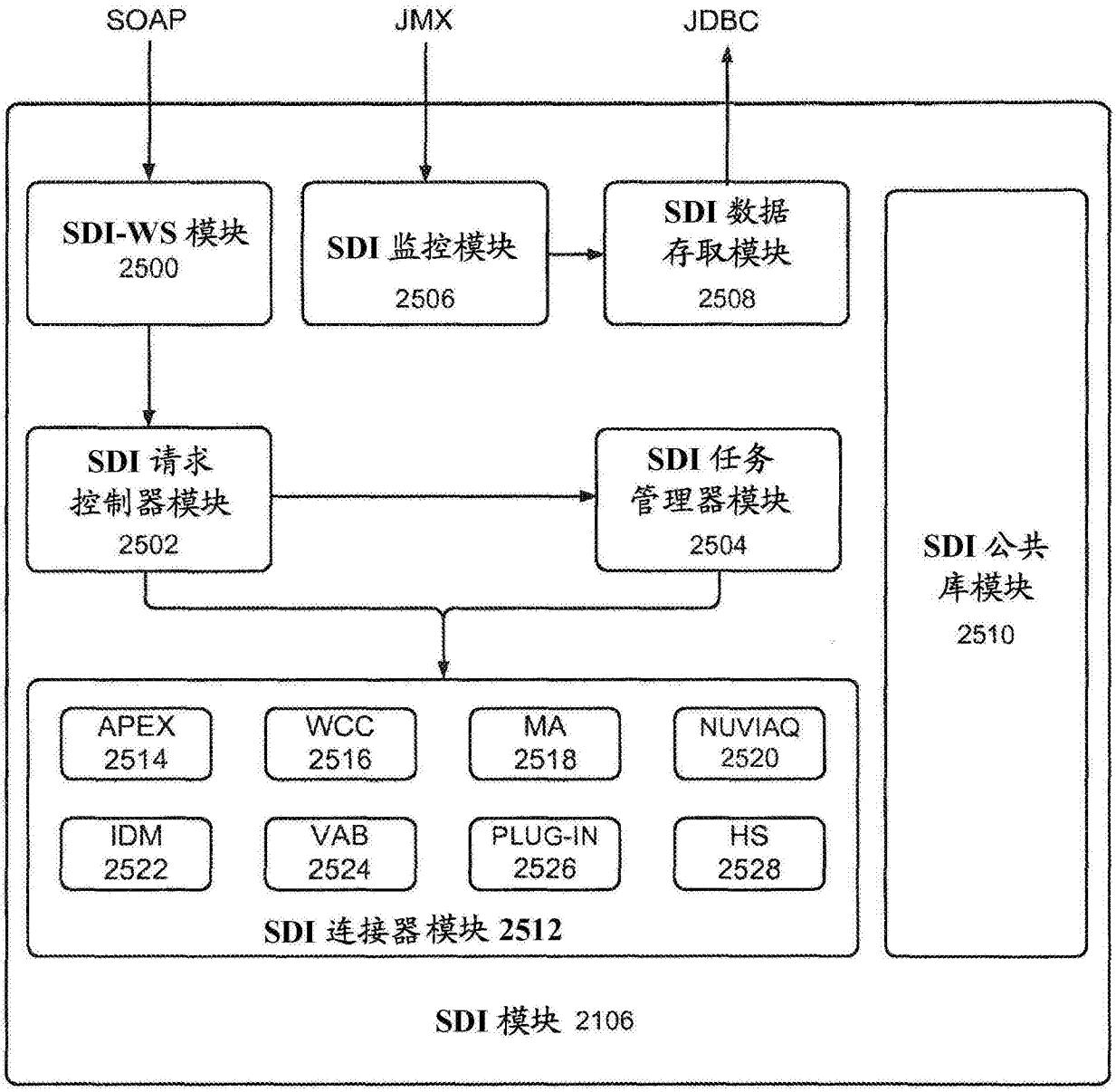

SOAP
JMX
JDBC
SDI-WS 模块
2500
SDI 监控模块
2506
SDI 数据
存取模块
2508
SDI 请求
控制器模块
2502
SDI 任务
管理器模块
2504
SDI 公共
库模块
2510
APEX
2514
WCC
2516
MA
2518
NUVIAQ
2520
IDM
2522
VAB
2524
PLUG-IN
2526
HS
2528
SDI 连接器模块 2512
SDI 模块 2106

图25

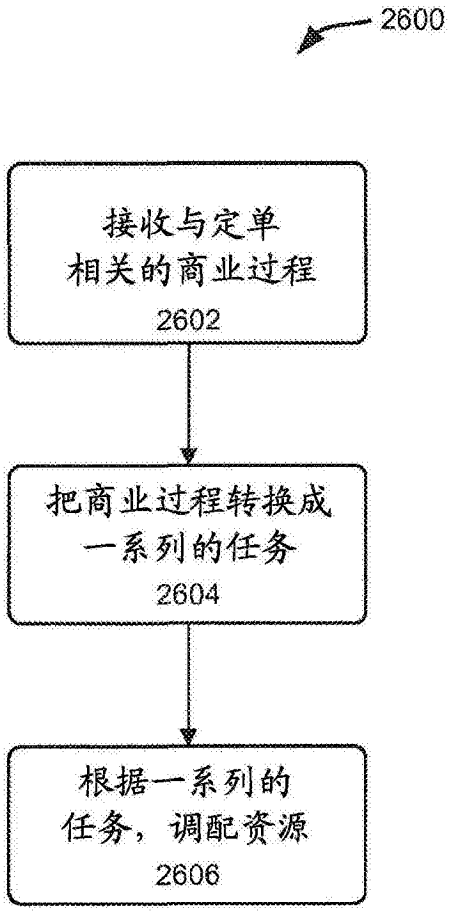

2600
接收与定单
相关的商业过程
2602
把商业过程转换成
一系列的任务
2604
根据一系列的
任务，调配资源
2606

图26A

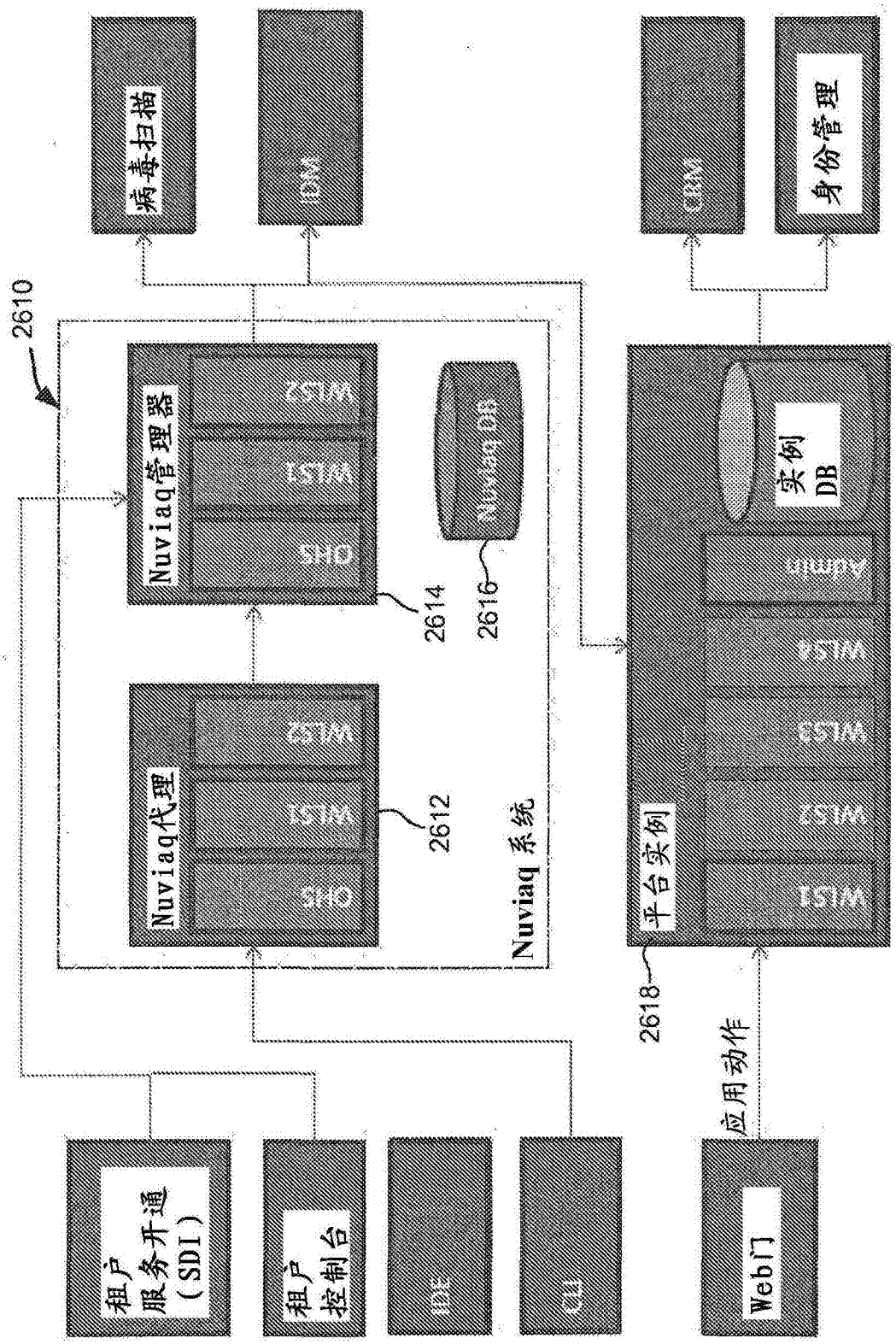

病毒扫描
IDM
CRM
身份管理
2610
Nuviaq管理器
WLS2
WLS1
OHS
2614
NuviaqDB
2616
实例DB
Admin
WLS4
WLS3
WLS2
WLS1
Nuviaq代理
WLS2
WLS1
OHS
2612
Nuviaq 系统
平台实例
2618
应用动作
租户服务开通（SDI）
租户控制台
IDE
CLI
Web门

图26B

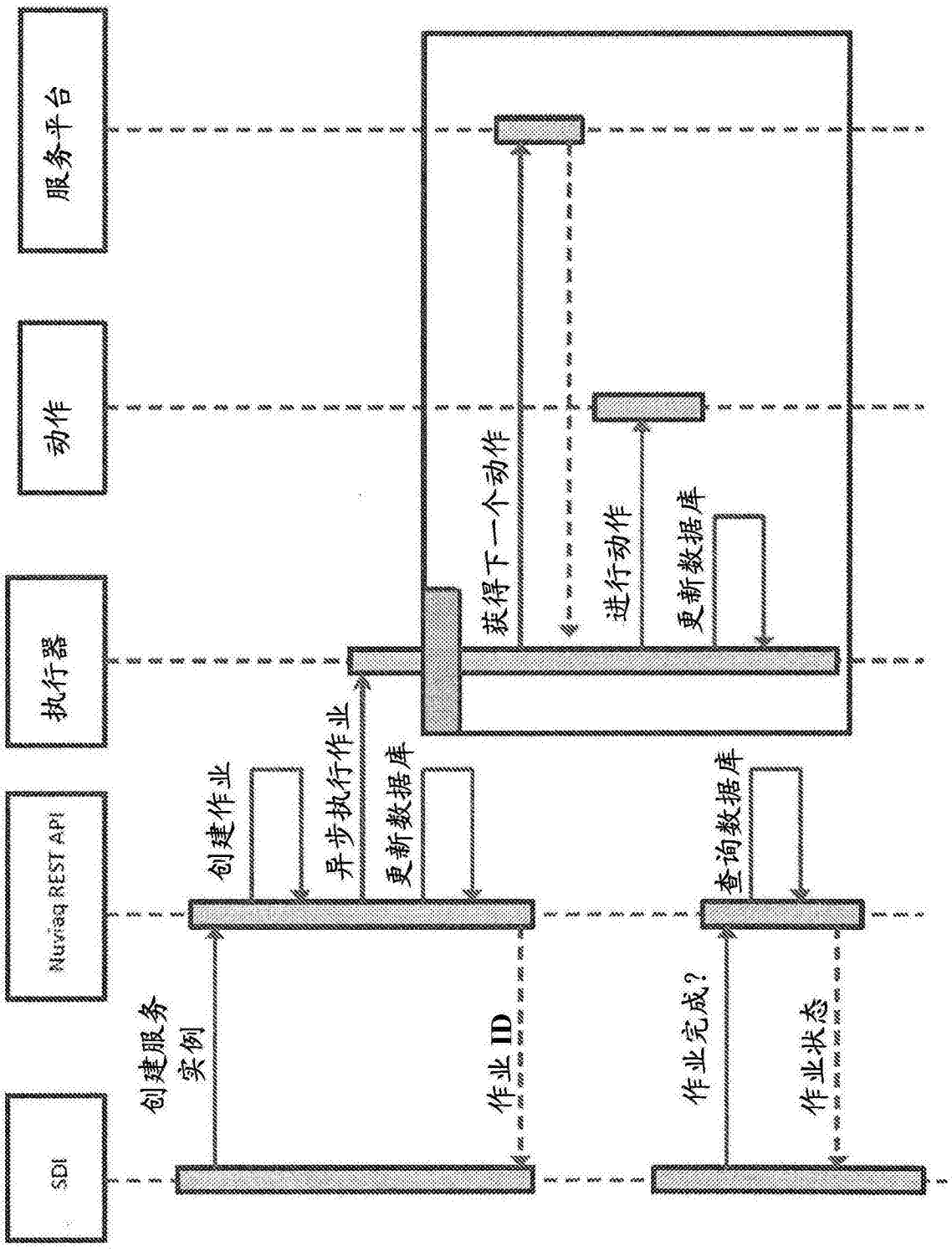

SDI
Nuwiaq REST API
执行器
动作
服务平台
创建服务实例
创建作业
异步执行作业
更新数据库
获得下一个动作
进行动作
更新数据库
作业 ID
作业完成？
查询数据库
作业状态

图26C

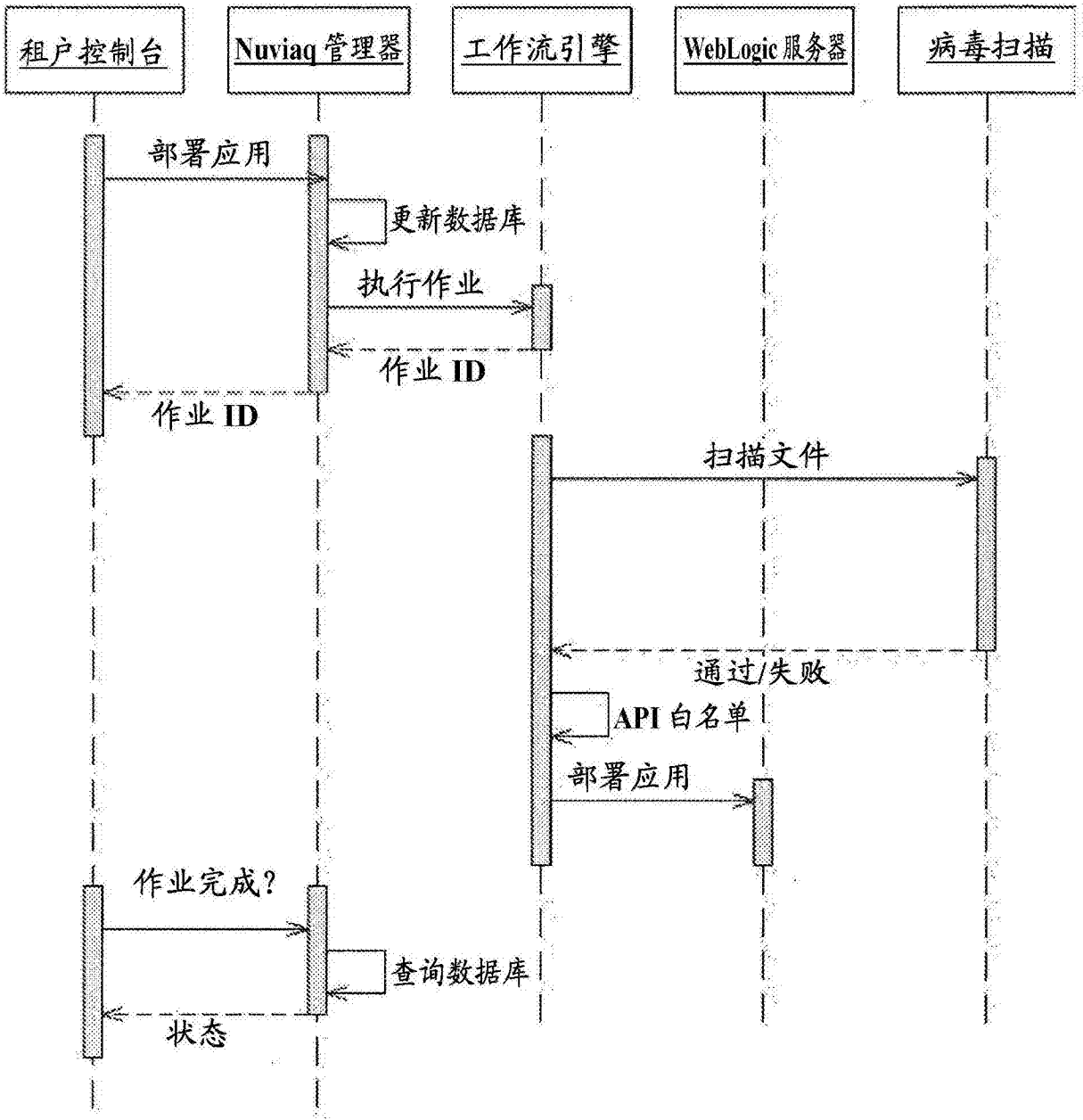

租户控制台
Nuviaq 管理器
工作流引擎
WebLogic 服务器
病毒扫描
部署应用
更新数据库
执行作业
作业 ID
作业 ID
扫描文件
通过/失败
API 白名单
部署应用
作业完成?
查询数据库
状态

图26D

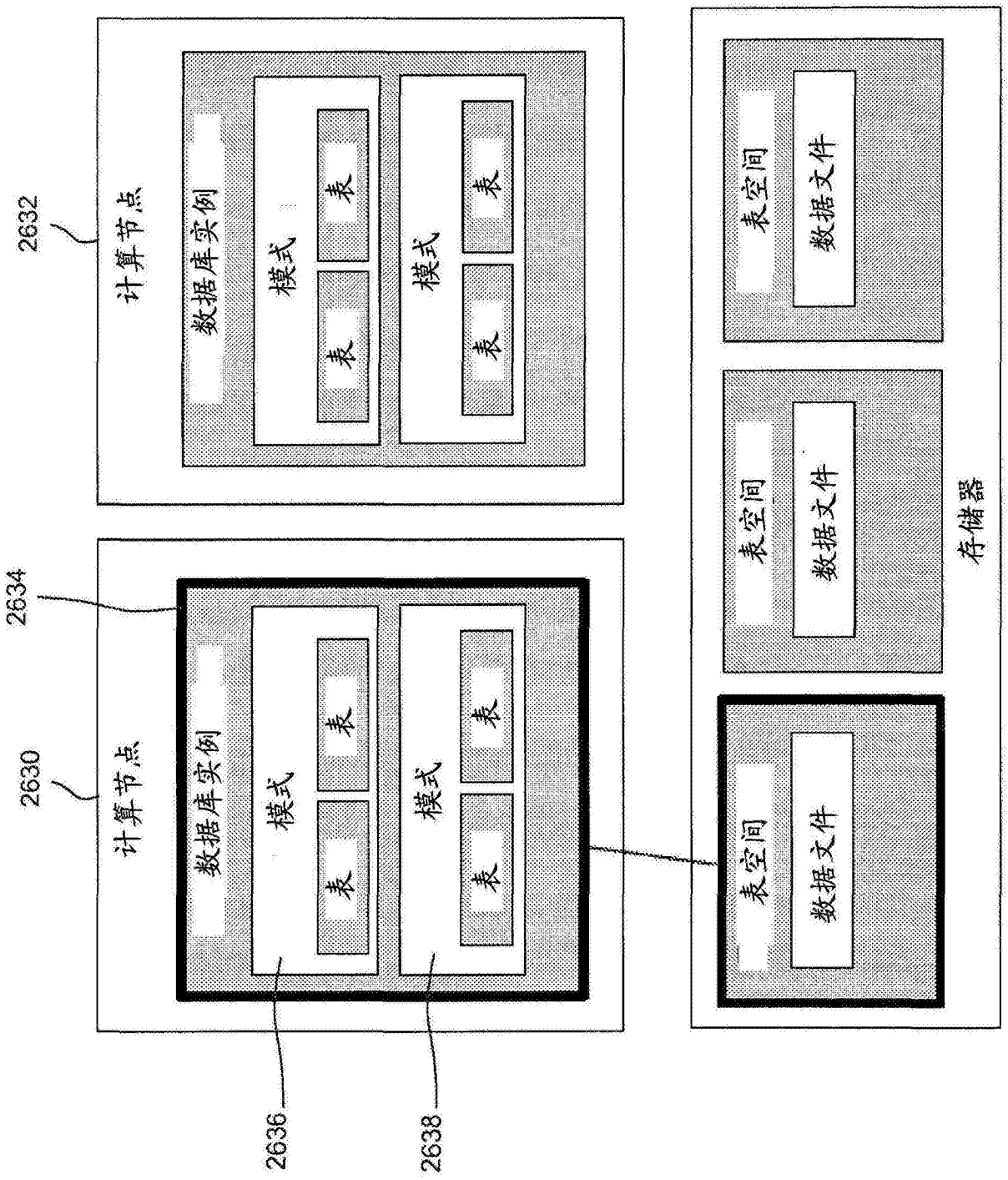

2632
计算节点
数据库实例
模式
表
表
模式
表
表
2634
2630
计算节点
数据库实例
模式
表
表
模式
表
表
2636
2638
表空间
数据文件
表空间
数据文件
表空间
数据文件
存储器

图26E

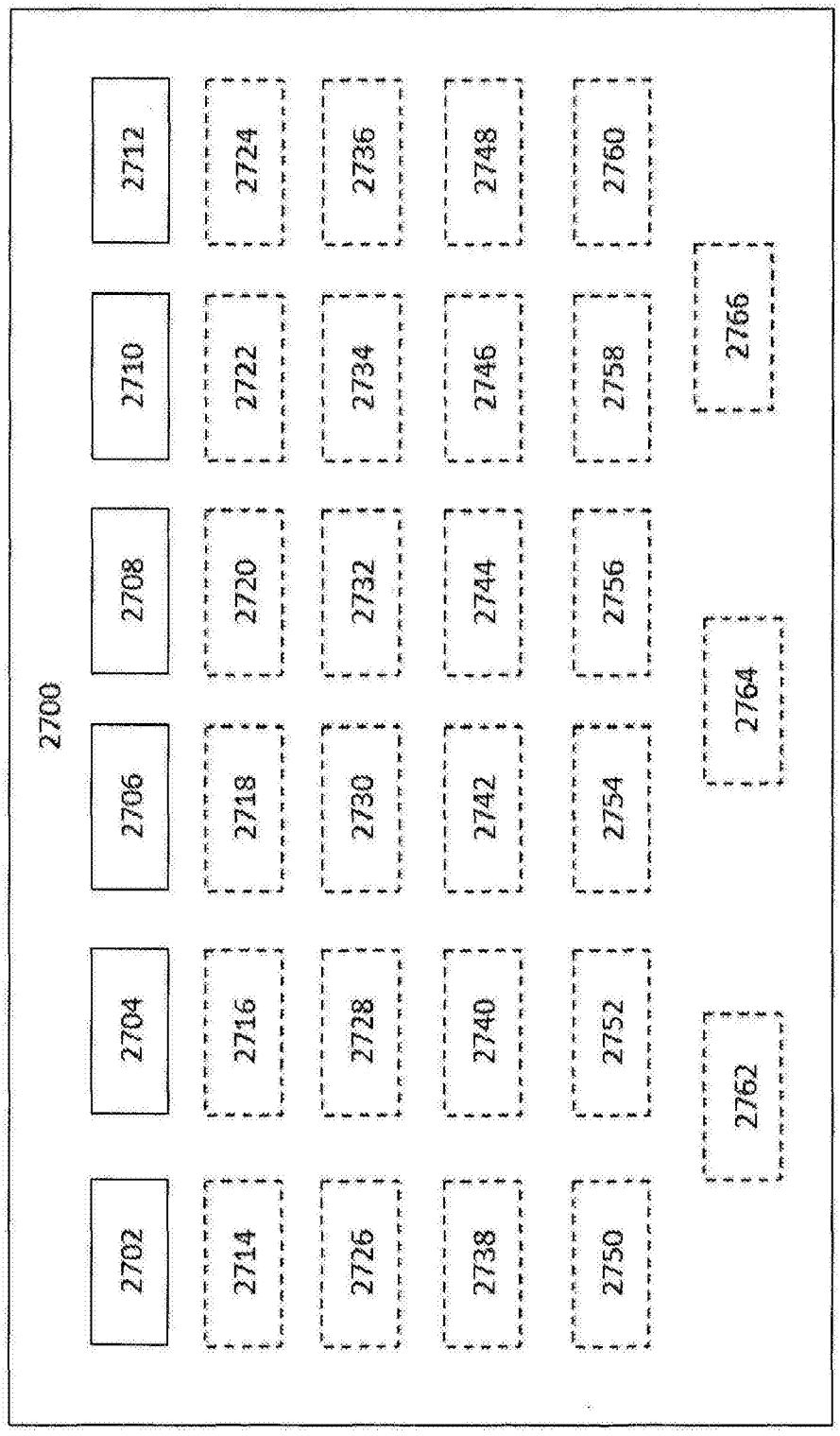

2700
2702
2704
2706
2708
2710
2712
2714
2716
2718
2720
2722
2724
2726
2728
2730
2732
2734
2736
2738
2740
2742
2744
2746
2748
2750
2752
2754
2756
2758
2760
2762
2764
2766

图27

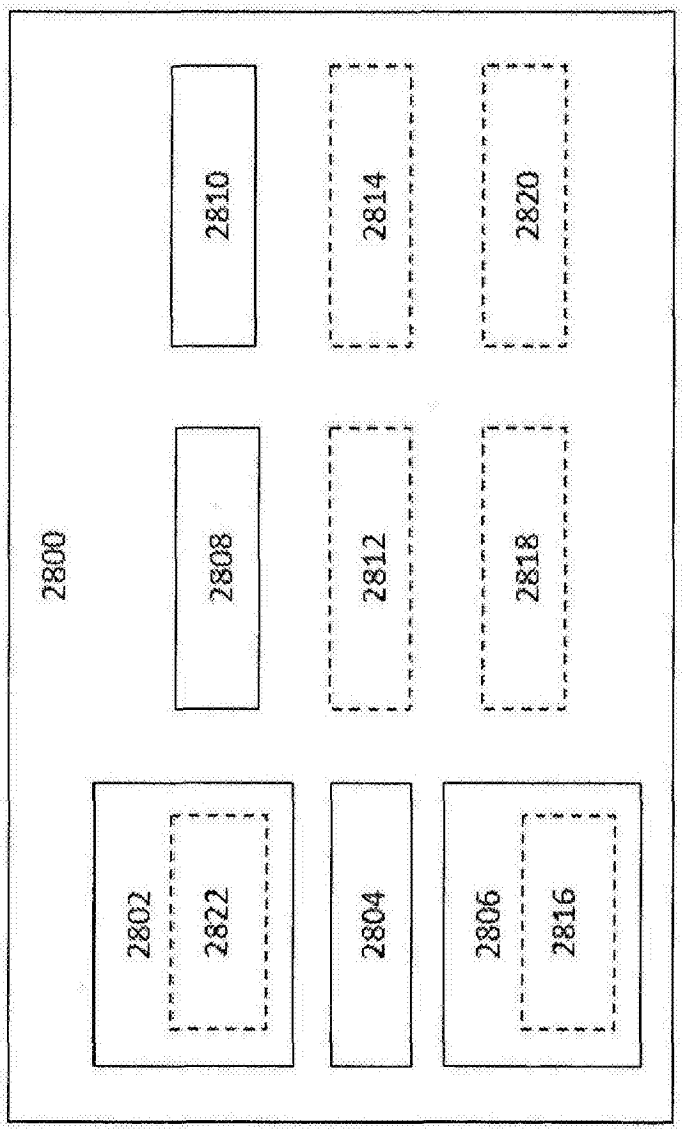


图28

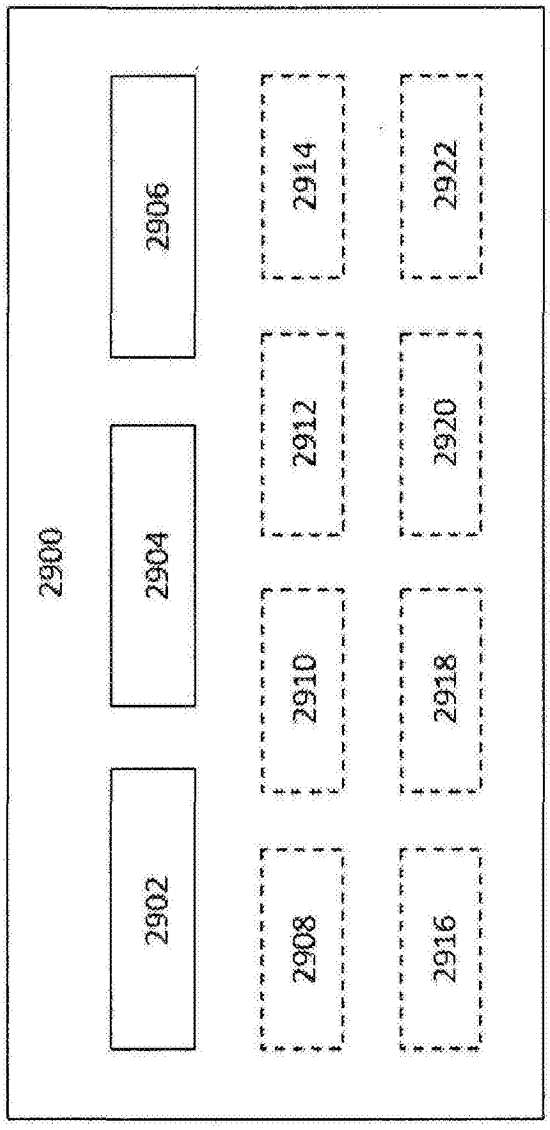


图29