



(12)发明专利申请

(10)申请公布号 CN 106302425 A

(43)申请公布日 2017. 01. 04

(21)申请号 201610647390.0

(22)申请日 2016.08.09

(71)申请人 浪潮(北京)电子信息产业有限公司

地址 100085 北京市海淀区上地信息路2号
2-1号C栋1层

(72)发明人 王永超

(74)专利代理机构 北京集佳知识产权代理有限公司 11227

代理人 罗满

(51)Int.Cl.

H04L 29/06(2006.01)

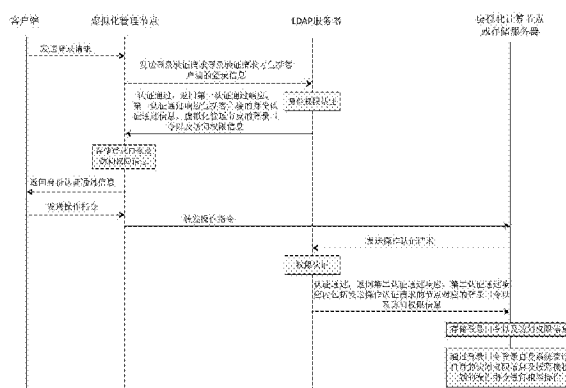
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种虚拟化系统节点间通信方法及其虚拟化系统

(57)摘要

本发明公开了一种虚拟化系统节点间通信方法,虚拟化管理节点接收到客户端发送的登录请求后,发送登录验证请求至LDAP服务器进行身份权限验证,验证通过后,接收LDAP服务器返回的登录口令以及访问权限信息;虚拟化计算节点或存储服务器首次接收到操作指令后,发送操作认证请求至LDAP服务器进行权限认证,认证通过后,接收LDAP服务器返回至自身的登录口令以及访问权限信息。本发明对登录口令进行了分散,各个节点分别存储自身的登录口令,而不是由虚拟化管理节点统一存储,故降低了各个虚拟化计算节点以及存储服务器的登录口令被破解的风险,安全性高。本发明的另一目的是提供一种虚拟化系统。



1. 一种虚拟化系统节点间通信方法,其特征在于,包括:

虚拟化管理节点接收客户端发送的登录请求后,发送登录验证请求至LDAP服务器进行身份权限认证;其中,所述登录验证请求内包括所述客户端的登录信息;

若认证通过,所述LDAP服务器返回第一认证通过响应至所述虚拟化管理节点;所述第一认证通过响应包括所述客户端的身份认证通过信息、所述虚拟化管理节点的登录口令以及访问权限信息;

所述虚拟化管理节点接收所述第一认证通过响应后,存储所述登录口令以及所述访问权限信息,并返回所述身份认证通过信息至所述客户端;

虚拟化计算节点或存储服务器首次接收到所述客户端通过所述虚拟化管理节点发送的操作指令后,发送操作认证请求至所述LDAP服务器进行权限认证;

若认证通过,所述LDAP服务器返回第二认证通过响应至发送所述操作认证请求的节点;其中,所述第二认证通过响应内包括发送所述操作认证请求的节点对应的登录口令以及访问权限信息;

所述虚拟化计算节点或所述存储服务器接收到所述第二认证通过响应后存储所述第二认证通过响应内的登录口令以及访问权限信息,并通过自身的登录口令登录自身系统后查询自身的访问权限信息以及按照接收到的所述操作指令进行相应操作。

2. 根据权利要求1所述的方法,其特征在于,所述虚拟化管理节点发送登录验证请求至LDAP服务器进行身份权限认证的过程具体为:

所述虚拟化管理节点发送所述登录验证请求至密钥分配中心;

所述密钥分配中心建立与所述虚拟化管理节点之间的安全通信通道以及开放与所述虚拟化管理节点之间的会话权限,并将所述登录验证请求发送至所述LDAP服务器进行身份权限认证。

3. 根据权利要求2所述的方法,其特征在于,所述虚拟化计算节点或所述存储服务器首次接收到所述操作指令后发送操作认证请求至所述LDAP服务器进行权限认证的过程具体为:

所述虚拟化计算节点或所述存储服务器首次接收到所述操作指令后发送所述操作认证请求至所述密钥分配中心;

所述密钥分配中心建立与所述虚拟化计算节点或所述存储服务器之间的安全通信通道以及开放与所述虚拟化计算节点或所述存储服务器之间的会话权限,并将所述登录验证请求发送至所述LDAP服务器进行权限认证。

4. 根据权利要求2或3所述的方法,其特征在于,所述密钥分配中心建立与相应节点之间的安全通信通道的过程具体为:

所述密钥分配中心分配一对公钥和私钥至所述相应节点,供所述相应节点接收数据信息时使用所述私钥解密,发送数据信息时使用所述公钥加密。

5. 根据权利要求4所述的方法,其特征在于,当所述虚拟化管理节点、所述虚拟化计算节点以及所述存储服务器均接收到所述密钥分配中心分配的一对公钥和私钥且均接收到所述LDAP服务器发送的登录口令后,还包括:

建立所述虚拟化管理节点与所述客户端之间、所述虚拟化管理节点与所述虚拟化计算节点之间、所述虚拟化管理节点与所述存储服务器之间以及所述虚拟化计算节点与所述存

储服务器之间的安全通信通道。

6. 一种虚拟化系统,其特征在於,包括虚拟化管理节点、虚拟化计算节点、存储服务器以及LDAP服务器;其中:

所述虚拟化管理节点,用于接收客户端发送的登录请求后,发送登录验证请求至LDAP服务器进行身份权限认证;其中,所述登录验证请求内包括所述客户端的登录信息;接收所述第一认证通过响应后,存储所述登录口令以及所述访问权限信息,并返回所述身份认证通过信息至所述客户端;

所述LDAP服务器,用于接收所述登录验证请求后进行认证,若认证通过,返回第一认证通过响应至所述虚拟化管理节点;所述第一认证通过响应包括所述客户端的身份认证通过信息、所述虚拟化管理节点的登录口令以及访问权限信息;接收到的操作认证请求后进行认证,若认证通过,返回第二认证通过响应至发送所述操作认证请求的节点;其中,所述第二认证通过响应内包括发送所述操作认证请求的节点对应的登录口令以及访问权限信息;

所述虚拟化计算节点以及所述存储服务器,用于当首次接收到所述客户端通过所述虚拟化管理节点发送的操作指令后,发送操作认证请求至所述LDAP服务器进行权限认证;接收到所述第二认证通过响应后存储所述第二认证通过响应内的登录口令以及访问权限信息,并通过自身的登录口令登录自身系统后查询自身的访问权限信息以及按照接收到的所述操作指令进行相应操作。

7. 根据权利要求6所述的系统,其特征在於,还包括:

密钥分配中心,用于接收所述虚拟化管理节点发送的所述登录验证请求,并建立与所述虚拟化管理节点之间的安全通信通道以及开放与所述虚拟化管理节点之间的会话权限,并将所述登录验证请求发送至所述LDAP服务器进行身份权限认证。

8. 根据权利要求7所述的系统,其特征在於,所述密钥分配中心还用于:

接收所述虚拟化计算节点或所述存储服务器首次接收到所述操作指令后发送的所述操作认证请求,并建立与所述虚拟化计算节点或所述存储服务器之间的安全通信通道以及开放与所述虚拟化计算节点或所述存储服务器之间的会话权限,并将所述登录验证请求发送至所述LDAP服务器进行权限认证。

一种虚拟化系统节点间通信方法及其虚拟化系统

技术领域

[0001] 本发明涉及虚拟化节点通信技术领域,特别是涉及一种虚拟化系统节点间通信方法。本发明还涉及一种虚拟化系统。

背景技术

[0002] 随着云计算技术以及虚拟化技术的飞速发展,虚拟化系统节点间的通信安全越来越成为社会发展的需要。

[0003] 目前的虚拟化系统中,虚拟化计算节点以及存储服务器的登录口令均存储于虚拟化管理节点内,且存储的登录口令一般通过算法得到,即可被人破解,故一旦虚拟化管理节点被攻击出现信息泄露,攻击者可以通过对泄露信息进行分析来获得虚拟化计算节点以及存储服务器的登录口令,进而控制虚拟化计算节点以及存储服务器,导致通信数据泄露,可见,目前的虚拟化节点间的通信方式安全性低,各个虚拟化计算节点以及存储服务器的登录口令被破解的风险高。

[0004] 因此,如何提供一种安全性高的虚拟化系统节点间通信方法及其虚拟化系统是本领域技术人员目前需要解决的问题。

发明内容

[0005] 本发明的目的是提供一种虚拟化系统节点间通信方法,降低了各个虚拟化计算节点以及存储服务器的登录口令被破解的风险,安全性高。本发明的另一目的是提供一种虚拟化系统。

[0006] 为解决上述技术问题,本发明提供了一种虚拟化系统节点间通信方法,包括:

[0007] 虚拟化管理节点接收客户端发送的登录请求后,发送登录验证请求至LDAP服务器进行身份权限认证;其中,所述登录验证请求内包括所述客户端的登录信息;

[0008] 若认证通过,所述LDAP服务器返回第一认证通过响应至所述虚拟化管理节点;所述第一认证通过响应包括所述客户端的身份认证通过信息、所述虚拟化管理节点的登录口令以及访问权限信息;

[0009] 所述虚拟化管理节点接收所述第一认证通过响应后,存储所述登录口令以及所述访问权限信息,并返回所述身份认证通过信息至所述客户端;

[0010] 虚拟化计算节点或存储服务器首次接收到所述客户端通过所述虚拟化管理节点发送的操作指令后,发送操作认证请求至所述LDAP服务器进行权限认证;

[0011] 若认证通过,所述LDAP服务器返回第二认证通过响应至发送所述操作认证请求的节点;其中,所述第二认证通过响应内包括发送所述操作认证请求的节点对应的登录口令以及访问权限信息;

[0012] 所述虚拟化计算节点或所述存储服务器接收到所述第二认证通过响应后存储所述第二认证通过响应内的登录口令以及访问权限信息,并通过自身的登录口令登录自身系统后查询自身的访问权限信息以及按照接收到的所述操作指令进行相应操作。

[0013] 优选地,所述虚拟化管理节点发送登录验证请求至LDAP服务器进行身份权限认证的过程具体为:

[0014] 所述虚拟化管理节点发送所述登录验证请求至密钥分配中心;

[0015] 所述密钥分配中心建立与所述虚拟化管理节点之间的安全通信通道以及开放与所述虚拟化管理节点之间的会话权限,并将所述登录验证请求发送至所述LDAP服务器进行身份权限认证。

[0016] 优选地,所述虚拟化计算节点或所述存储服务器首次接收到所述操作指令后发送操作认证请求至所述LDAP服务器进行权限认证的过程具体为:

[0017] 所述虚拟化计算节点或所述存储服务器首次接收到所述操作指令后发送所述操作认证请求至所述密钥分配中心;

[0018] 所述密钥分配中心建立与所述虚拟化计算节点或所述存储服务器之间的安全通信通道以及开放与所述虚拟化计算节点或所述存储服务器之间的会话权限,并将所述登录验证请求发送至所述LDAP服务器进行权限认证。

[0019] 优选地,所述密钥分配中心建立与相应节点之间的安全通信通道的过程具体为:

[0020] 所述密钥分配中心分配一对公钥和私钥至所述相应节点,供所述相应节点接收数据信息时使用所述私钥解密,发送数据信息时使用所述公钥加密。

[0021] 优选地,当所述虚拟化管理节点、所述虚拟化计算节点以及所述存储服务器均接收到所述密钥分配中心分配的一对公钥和私钥且均接收到所述LDAP服务器发送的登录口令后,还包括:

[0022] 建立所述虚拟化管理节点与所述客户端之间、所述虚拟化管理节点与所述虚拟化计算节点之间、所述虚拟化管理节点与所述存储服务器之间以及所述虚拟化计算节点与所述存储服务器之间的安全通信通道。

[0023] 为解决上述技术问题,本发明还提供了一种虚拟化系统,包括虚拟化管理节点、虚拟化计算节点、存储服务器以及LDAP服务器;其中:

[0024] 所述虚拟化管理节点,用于接收客户端发送的登录请求后,发送登录验证请求至LDAP服务器进行身份权限认证;其中,所述登录验证请求内包括所述客户端的登录信息;接收所述第一认证通过响应后,存储所述登录口令以及所述访问权限信息,并返回所述身份认证通过信息至所述客户端;

[0025] 所述LDAP服务器,用于接收所述登录验证请求后进行认证,若认证通过,返回第一认证通过响应至所述虚拟化管理节点;所述第一认证通过响应包括所述客户端的身份认证通过信息、所述虚拟化管理节点的登录口令以及访问权限信息;接收到的操作认证请求后进行认证,若认证通过,返回第二认证通过响应至发送所述操作认证请求的节点;其中,所述第二认证通过响应内包括发送所述操作认证请求的节点对应的登录口令以及访问权限信息;

[0026] 所述虚拟化计算节点以及所述存储服务器,用于当首次接收到所述客户端通过所述虚拟化管理节点发送的操作指令后,发送操作认证请求至所述LDAP服务器进行权限认证;接收到所述第二认证通过响应后存储所述第二认证通过响应内的登录口令以及访问权限信息,并通过自身的登录口令登录自身系统后查询自身的访问权限信息以及按照接收到的所述操作指令进行相应操作。

[0027] 优选地,还包括:

[0028] 密钥分配中心,用于接收所述虚拟化管理节点发送的所述登录验证请求,并建立与所述虚拟化管理节点之间的安全通信通道以及开放与所述虚拟化管理节点之间的会话权限,并将所述登录验证请求发送至所述LDAP服务器进行身份权限认证。

[0029] 优选地,所述密钥分配中心还用于:

[0030] 接收所述虚拟化计算节点或所述存储服务器首次接收到所述操作指令后发送的所述操作认证请求,并建立与所述虚拟化计算节点或所述存储服务器之间的安全通信通道以及开放与所述虚拟化计算节点或所述存储服务器之间的会话权限,并将所述登录验证请求发送至所述LDAP服务器进行权限认证。

[0031] 本发明提供了一种虚拟化系统节点间通信方法,虚拟化管理节点、虚拟化计算节点以及存储服务器的登录口令以及访问权限均由LDAP服务器进行认证后分配,即本发明对登录口令进行了分散,各个节点分别存储自身的登录口令,而不是由虚拟化管理节点统一存储,故即使虚拟化管理节点被攻击出现信息泄露,攻击者也无法获取虚拟化计算节点以及存储服务器的登录口令;并且,以上各个节点的登录口令均由LDAP服务器进行分配,该种登录口令不可逆推,即无法通过算法计算破解登录口令,可见,本发明安全性高,各个虚拟化计算节点以及存储服务器的登录口令被破解的风险低。本发明还提供了一种虚拟化系统,也具有上述优点,在此不再赘述。

附图说明

[0032] 为了更清楚地说明本发明实施例中的技术方案,下面将对现有技术和实施例中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0033] 图1为本发明提供的一种虚拟化系统节点间通信方法的过程的流程图;

[0034] 图2为本发明提供的一种虚拟化系统的结构示意图。

具体实施方式

[0035] 本发明的核心是提供一种虚拟化系统节点间通信方法,降低了各个虚拟化计算节点以及存储服务器的登录口令被破解的风险,安全性高。本发明的另一核心是提供一种虚拟化系统。

[0036] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0037] 本发明提供了一种虚拟化系统节点间通信方法,参见图1所示,图1为本发明提供的一种虚拟化系统节点间通信方法的过程的流程图;包括:

[0038] 虚拟化管理节点接收客户端发送的登录请求后,发送登录验证请求至LDAP服务器进行身份权限认证;其中,登录验证请求内包括客户端的登录信息;

[0039] 若认证通过,LDP服务器返回第一认证通过响应至虚拟化管理节点;第一认证通

过响应包括客户端的身份认证通过信息、虚拟化管理节点的登录口令以及访问权限信息；

[0040] 虚拟化管理节点接收第一认证通过响应后，存储登录口令以及访问权限信息，并返回身份认证通过信息至客户端；

[0041] 虚拟化计算节点或存储服务器首次接收到客户端通过虚拟化管理节点发送的操作指令后，发送操作认证请求至LDAP服务器进行权限认证；

[0042] 需要注意的是，虚拟化计算节点或存储服务器接收的操作指令可能不是由虚拟化管理节点直接发送的，而是由虚拟化管理节点发送至其他虚拟化计算节点，再由其他虚拟化计算节点转发至虚拟化计算节点或存储服务器。上述操作表明的是，只要虚拟化计算节点或存储服务器首次接收到操作指令，则要通过LDAP服务器进行权限认证。

[0043] 若认证通过，LDAP服务器返回第二认证通过响应至发送操作认证请求的节点；其中，第二认证通过响应内包括发送操作认证请求的节点对应的登录口令以及访问权限信息；

[0044] 虚拟化计算节点或存储服务器接收到第二认证通过响应后存储第二认证通过响应内的登录口令以及访问权限信息，并通过自身的登录口令登录自身系统后查询自身的访问权限信息以及按照接收到的操作指令进行相应操作。

[0045] 其中，这里的登录口令具体为身份识别令牌(Token)。

[0046] 另外，虚拟化计算节点与存储服务器之间也有连接，虚拟化计算节点可以调用存储服务器内的数据或者将自身得到的数据存储至存储服务器内。

[0047] 可以理解的是，LDAP(Lightweight Directory Access Protocol,轻量目录访问协议)服务器具有对域内物理节点充分授权和资源管理的特点，LDAP服务器指的是采用LDAP协议通信的服务器，作为优选地，本发明中的LDAP服务器采用Kerberos认证技术进行认证操作。

[0048] 另外，本发明中对用户登录时的身份验证操作由LDAP服务器进行，而不再由虚拟化管理节点进行，故虚拟化管理节点内不再需要存储与用户登录信息相关的敏感数据，提高了用户登录信息数据的安全性。

[0049] 作为优选地，虚拟化管理节点发送登录验证请求至LDAP服务器进行身份权限认证的过程具体为：

[0050] 虚拟化管理节点发送登录验证请求至密钥分配中心；

[0051] 密钥分配中心建立与虚拟化管理节点之间的安全通信通道以及开放与虚拟化管理节点之间的会话权限，并将登录验证请求发送至LDAP服务器进行身份权限认证。

[0052] 进一步的，虚拟化计算节点或存储服务器首次接收到操作指令后发送操作认证请求至LDAP服务器进行权限认证的过程具体为：

[0053] 虚拟化计算节点或存储服务器首次接收到操作指令后发送操作认证请求至密钥分配中心；

[0054] 密钥分配中心建立与虚拟化计算节点或存储服务器之间的安全通信通道以及开放与虚拟化计算节点或存储服务器之间的会话权限，并将登录验证请求发送至LDAP服务器进行权限认证。

[0055] 可以理解的是，在尚未建立安全通信通道时，各个节点通过初始通道进行通信。

[0056] 其中，密钥分配中心建立与相应节点之间的安全通信通道的过程具体为：

[0057] 密钥分配中心分配一对公钥和私钥至相应节点,供相应节点接收数据信息时使用私钥解密,发送数据信息时使用公钥加密。

[0058] 可以理解的是,通过采用上述加密解密方式,可以尽可能保证通信通道的可靠性及安全性,即可理解为建立了安全的通信通道。

[0059] 进一步的,当虚拟化管理节点、虚拟化计算节点以及存储服务器均接收到密钥分配中心分配的一对公钥和私钥且均接收到LDAP服务器发送的登录口令后,还包括:

[0060] 建立虚拟化管理节点与客户端之间、虚拟化管理节点与虚拟化计算节点之间、虚拟化管理节点与存储服务器之间以及虚拟化计算节点与存储服务器之间的安全通信通道。

[0061] 另外,当各个节点均通过LDAP服务器的权限认证后,当虚拟化管理节点或虚拟化计算节点或存储服务器再次接收到客户端发送的操作指令后,则首先通过自身的登录口令登录自身系统,查询访问权限信息,若操作属于自身权限范围内,则执行该操作内容,否则,经该操作指令转发至相应的虚拟化计算节点或存储服务器。

[0062] 本发明提供了一种虚拟化系统节点间通信方法,虚拟化管理节点、虚拟化计算节点以及存储服务器的登录口令以及访问权限均由LDAP服务器进行认证后分配,即本发明对登录口令进行了分散,各个节点分别存储自身的登录口令,而不是由虚拟化管理节点统一存储,故即使虚拟化管理节点被攻击出现信息泄露,攻击者也无法获取虚拟化计算节点以及存储服务器的登录口令;并且,以上各个节点的登录口令均由LDAP服务器进行分配,该种登录口令不可逆推,即无法通过算法计算破解登录口令,可见,本发明安全性高,各个虚拟化计算节点以及存储服务器的登录口令被破解的风险低。

[0063] 本发明还提供了一种虚拟化系统,参见图2所示,图2为本发明提供的一种虚拟化系统的结构示意图。该系统包括虚拟化管理节点11、虚拟化计算节点12、存储服务器13以及LDAP服务器14;其中:

[0064] 虚拟化管理节点11,用于接收客户端发送的登录请求后,发送登录验证请求至LDAP服务器14进行身份权限认证;其中,登录验证请求内包括客户端的登录信息;接收第一认证通过响应后,存储登录口令以及访问权限信息,并返回身份认证通过信息至客户端;

[0065] LDAP服务器14,用于接收登录验证请求后进行认证,若认证通过,返回第一认证通过响应至虚拟化管理节点11;第一认证通过响应包括客户端的身份认证通过信息、虚拟化管理节点11的登录口令以及访问权限信息;接收到的操作认证请求后进行认证,若认证通过,返回第二认证通过响应至发送操作认证请求的节点;其中,第二认证通过响应内包括发送操作认证请求的节点对应的登录口令以及访问权限信息;

[0066] 虚拟化计算节点12以及存储服务器13,用于当首次接收到客户端通过虚拟化管理节点11发送的操作指令后,发送操作认证请求至LDAP服务器14进行权限认证;接收到第二认证通过响应后存储第二认证通过响应内的登录口令以及访问权限信息,并通过自身的登录口令登录自身系统后查询自身的访问权限信息以及按照接收到的操作指令进行相应操作。

[0067] 作为优选地,还包括:

[0068] 密钥分配中心15,用于接收虚拟化管理节点11发送的登录验证请求,并建立与虚拟化管理节点11之间的安全通信通道以及开放与虚拟化管理节点11之间的会话权限,并将登录验证请求发送至LDAP服务器14进行身份权限认证。

[0069] 进一步的,密钥分配中心15还用于:

[0070] 接收虚拟化计算节点12或存储服务器13首次接收到操作指令后发送的操作认证请求,并建立与虚拟化计算节点12或存储服务器13之间的安全通信通道以及开放与虚拟化计算节点12或存储服务器13之间的会话权限,并将登录验证请求发送至LDAP服务器14进行权限认证。

[0071] 另外,该系统还包括交换机,该交换机分别与客户端、虚拟化管理节点11、虚拟化计算节点12以及存储服务器13相连,用于控制以上各个系统节点之间的数据交换,由于各个系统节点之间可能会不方便直接连接,故通过交换机能够方便的实现节点间通信。

[0072] 同时,本发明不限定虚拟化计算节点12以及存储服务器13的个数。

[0073] 本发明提供了一种虚拟化系统,虚拟化管理节点、虚拟化计算节点以及存储服务器的登录口令以及访问权限均由LDAP服务器进行认证后分配,即本发明对登录口令进行了分散,各个节点分别存储自身的登录口令,而不是由虚拟化管理节点统一存储,故即使虚拟化管理节点被攻击出现信息泄露,攻击者也无法获取虚拟化计算节点以及存储服务器的登录口令;并且,以上各个节点的登录口令均由LDAP服务器进行分配,该种登录口令不可逆推,即无法通过算法计算破解登录口令,可见,本发明安全性高,各个虚拟化计算节点以及存储服务器的登录口令被破解的风险低。

[0074] 需要说明的是,在本说明书中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0075] 对所公开的实施例的上述说明,使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的,本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下,在其他实施例中实现。因此,本发明将不会被限制于本文所示的这些实施例,而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

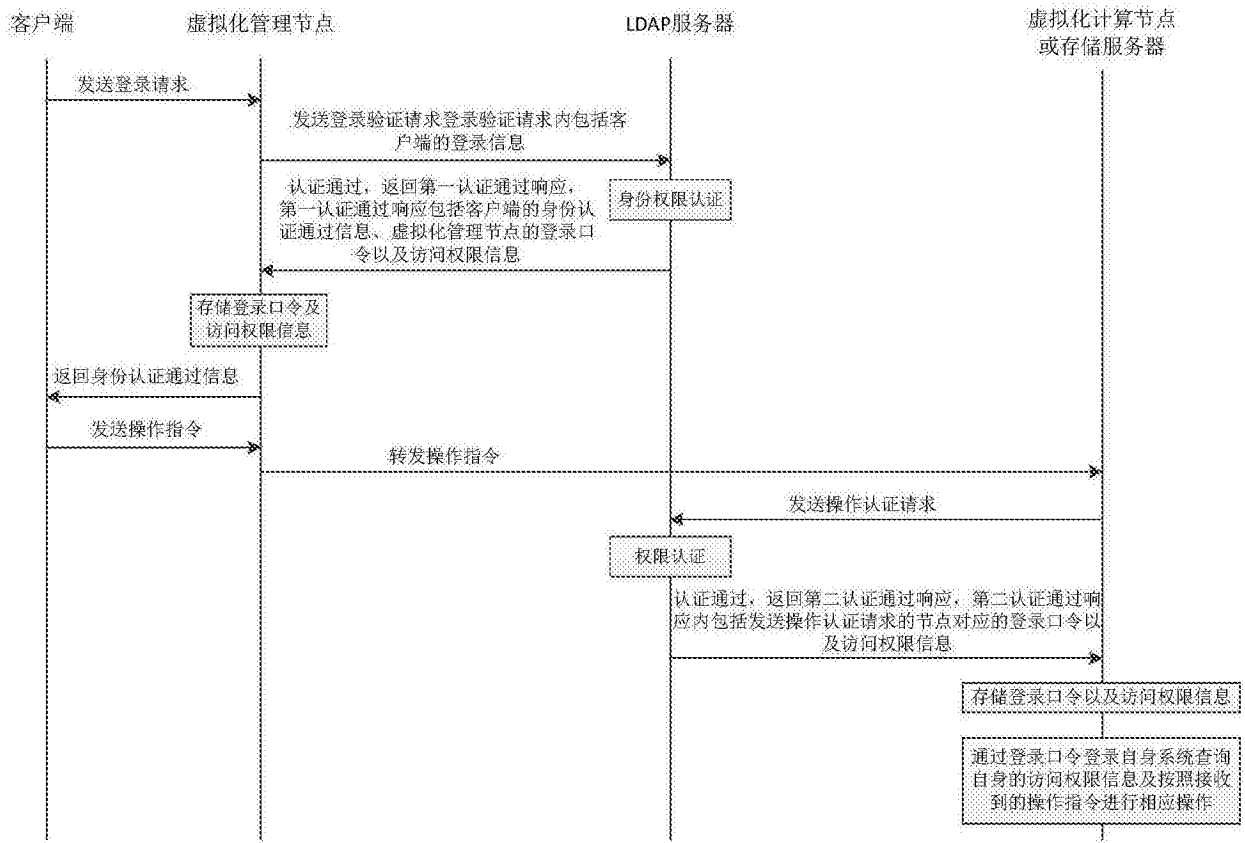


图1

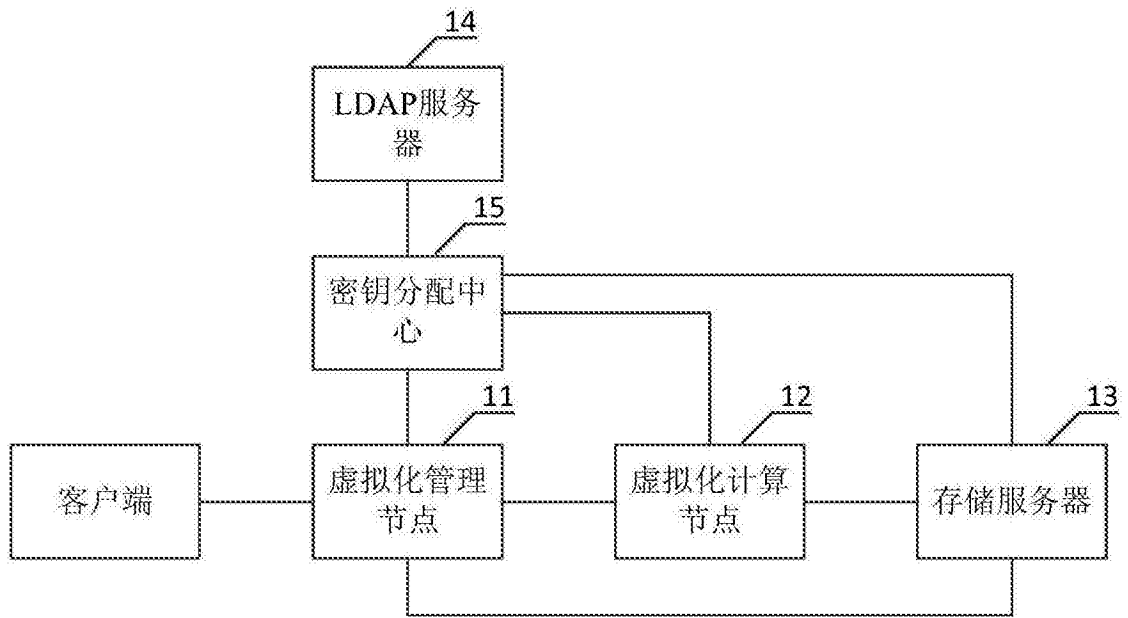


图2