(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 103399909 B
(45)授权公告日 2017.06.06

(21)申请号 201310325948.X

(22)申请日 2005.08.10

(65)同一申请的已公布的文献号
申请公布号 CN 103399909 A

(43)申请公布日 2013.11.20

(30)优先权数据
10/711730 2004.09.30 US
10/956832 2004.10.01 US
10/956764 2004.10.01 US

(62)分案原申请数据
200580041061.1 2005.08.10

(73)专利权人 茨特里克斯系统公司
地址 美国佛罗里达州

(72)发明人 R.G.布拉迪 T.西蒙斯
A.D.库克里尔 P.N.卡尔文

(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 郑冀之 刘春元

(51)Int.Cl.
G06F 17/30(2006.01)

(56)对比文件
CN 1363894 A,2002.08.14,
US 2004215826 A1,2004.10.28,
US 2004039594 A1,2004.02.26,
王燕平."Novell Intranetware 4 .11 服务器文件系统访问安全控制".《微机发展》.1999,(第5期),全部.

审查员 郭明亮

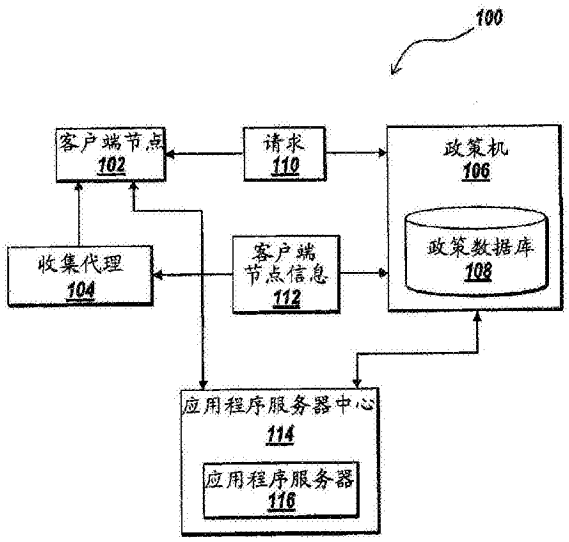
权利要求书3页 说明书17页 附图9页

(54)发明名称

在提供访问联网内容文件中分配访问控制级的方法和设备

(57)摘要

公开了当提供访问联网内容文件时,用于分配访问控制级的方法和设备,该设备包括客户端节点(102)、收集代理(104)、以及政策机(106)。客户端节点请求访问资源。收集代理收集关于该客户端节点的信息。政策机接收所收集的信息并且响应于政策的应用程序分配多个访问级之一给所接收的信息。应用程序服务器中心(114)可以使用与所请求的文件的文件类型有关的应用程序将资源内容呈现给客户端节点。转换服务器(516)可以将资源内容从原始格式转换为第二格式并且将所转换的资源内容呈现给客户端节点。



CN 103399909 B

1.一种提供文件内容的方法，包括：

访问控制服务器接收来自客户端节点的对于具有本地文件类型的文件的请求；

访问控制服务器做出访问控制决定来判定对于所述文件内容许可给客户端节点的访问等级；

响应于所判定的访问等级的访问控制服务器对客户端节点传送第二文件，第二文件可由客户端节点执行并且具有与所请求文件的本地文件类型不同的文件类型；

经由在客户端节点上的第二文件的执行建立到应用程序服务器的连接；以及

通过在所述应用程序服务器上执行的应用程序将文件内容经由所建立的连接呈现给所述客户端节点。

2.根据权利要求1的方法，进一步包括响应于访问等级从应用程序服务器中心识别所述应用程序服务器。

3.根据权利要求1的方法，进一步包括所述应用程序服务器识别与所述本地文件类型有关的应用程序。

4.根据权利要求2的方法，其中识别所述应用程序服务器进一步包括识别响应于所述访问等级的应用程序服务器。

5.根据权利要求1的方法，进一步包括从应用程序服务器中心识别第二应用程序服务器用于将文件内容呈现给所述客户端节点。

6.根据权利要求1的方法，进一步包括访问控制服务器基于所述访问等级生成所述第二文件。

7.根据权利要求6的方法，进一步包括从应用程序服务器中心识别第二应用程序服务器，所述第二应用程序服务器与所述文件的第二文件类型有关。

8.根据权利要求3的方法，其中识别所述应用程序进一步包括应用程序服务器，识别应用程序的标识符。

9.根据权利要求1的方法，进一步包括判定所请求文件的本地文件类型。

10.根据权利要求1的方法，进一步包括访问控制服务器获取关于所述客户端节点的信息。

11.根据权利要求10的方法，其中做出访问控制决定进一步包括比较由所述访问控制服务器获取的信息与政策以做出所述访问控制决定。

12.根据权利要求10的方法，其中呈现文件内容进一步包括所述应用程序服务器使用所获取的信息来选择用于呈现文件内容的格式。

13.根据权利要求10的方法，其中呈现文件内容进一步包括通过将政策应用到所获取的信息来呈现文件内容以选择用于呈现所述文件内容的格式。

14.根据权利要求1的方法，进一步包括访问控制服务器传送收集代理给所述客户端节点。

15.根据权利要求1的方法，进一步包括访问控制服务器使用收集代理获取关于所述客户端节点的信息。

16.根据权利要求15的方法，其中做出访问控制决定进一步包括比较由所述收集代理获取的信息与政策以做出访问控制决定。

17.根据权利要求1的方法，其中做出访问控制决定进一步包括访问控制服务器拒绝所

述请求。

18.根据权利要求9的方法，其中判定本地文件类型进一步包括访问控制服务器通过提取文件扩展名判定所述本地文件类型。

19.根据权利要求3的方法，其中识别应用程序进一步包括所述应用程序服务器通过使用所请求文件的文件扩展名查询用于该应用程序的数据库来识别所述应用程序。

20.根据权利要求1的方法，进一步包括从文件服务器取回所述文件。

21.根据权利要求20的方法，进一步包括应用程序服务器从文件服务器取回所述文件。

22.根据权利要求1的方法，进一步包括从web服务器取回所述文件。

23.根据权利要求22的方法，进一步包括应用程序服务器从web服务器取回所述文件。

24.根据权利要求22的方法，进一步包括访问控制服务器从web服务器取回所述文件。

25.根据权利要求1的方法，进一步包括从电子邮件服务器取回所述文件。

26.根据权利要求25的方法，进一步包括应用程序服务器从电子邮件服务器取回所述文件。

27.根据权利要求25的方法，进一步包括访问控制服务器从电子邮件服务器取回所述文件。

28.根据权利要求1的方法，进一步包括所述客户端节点连接到所述应用程序服务器。

29.根据权利要求28的方法，其中呈现文件内容进一步包括通过所述连接将所述文件内容呈现给所述客户端节点。

30.根据权利要求1的方法，其中传送第二文件进一步包括所述访问控制服务器传送可执行文件给所述客户端节点。

31.根据权利要求30的方法，进一步包括可执行文件识别用于将所述文件内容呈现给所述客户端节点的所述应用程序服务器。

32.根据权利要求1的方法，其中传送文件请求进一步包括所述客户端节点位于通过网络边界与第二网络分隔开的第一网络上，所述客户端节点从所述访问控制服务器请求文件，所述访问控制服务器位于所述第二网络上。

33.根据权利要求6的方法，其中判定所述本地文件类型进一步包括访问控制服务器从内容服务器下载所述文件。

34.根据权利要求1的方法，其中呈现所述文件内容进一步包括：

使用所述应用程序的标识符来识别所述应用程序服务器；

连接到所识别的应用程序服务器；以及

以所述应用程序服务器所选择的格式将文件内容呈现给所述客户端节点。

35.根据权利要求7的方法，其中所述第二文件类型不同于所述本地文件类型。

36.根据权利要求30的方法，进一步包括通过所述第二文件识别用于将文件内容呈现给所述客户端节点的应用程序。

37.一种用于提供文件内容的系统，包括：

访问控制服务器，其接收来自客户端节点的对于具有本地文件类型的文件的请求，做出访问控制决定来判定对于所述文件内容许可给客户端节点的访问等级，并且响应于所判定的访问等级对客户端节点传送第二文件，第二文件可由客户端节点执行并且具有与所请求文件的本地文件类型不同的文件类型，其中经由在客户端节点上的第二文件的执行建立

到应用程序服务器的连接；

以及

在所述应用程序服务器上执行的应用程序，其将文件内容经由所建立的连接呈现给所述客户端节点。

38.根据权利要求37的系统，其中所述应用程序服务器进一步识别与所述本地文件类型有关的应用程序。

39.根据权利要求37的系统，其中所述访问控制服务器进一步识别与所述本地文件类型有关的应用程序。

40.根据权利要求37的系统，其中所述访问控制服务器进一步包括存储至少一个政策的数据库。

41.根据权利要求37的系统，其中所述访问控制服务器进一步包括获取关于客户端节点的信息的收集代理。

42.根据权利要求41的系统，其中所述访问控制服务器基于由所述收集代理获取的信息做出访问控制决定以判定许可客户端节点访问所述文件内容的访问等级。

43.根据权利要求41的系统，其中所述访问控制服务器通过应用政策到由所述收集代理获取的信息做出访问控制决定以判定许可客户端节点访问所述文件内容的访问等级。

44.根据权利要求41的系统，其中所述收集代理获取关于客户端节点的有关所述客户端节点的设备类型的信息。

45.根据权利要求41的系统，其中所述收集代理获取关于客户端节点的有关网络连接信息的信息。

46.根据权利要求41的系统，其中所述收集代理获取关于客户端节点的有关授权证书的信息。

47.根据权利要求37的系统，其中所述应用程序服务器包括数据库，该数据库包含与至少一个文件类型有关的至少一个应用程序。

48.根据权利要求47的系统，其中所述应用程序服务器进一步通过查询所述数据库识别应用程序。

49.根据权利要求37的系统，其中所述访问控制服务器基于所判定的访问等级生成第二文件以传送给所述客户端节点。

50.根据权利要求49的系统，其中所述第二文件包括与所述本地文件类型有关的所述应用程序的标识符。

51.根据权利要求49的系统，其中所述第二文件识别所述应用程序服务器。

52.根据权利要求49的系统，其中所述客户端节点响应于接收到所述第二文件执行所述第二文件。

53.根据权利要求49的系统，其中所述应用程序服务器接受来自所述客户端节点的连接。

54.根据权利要求49的系统，其中所述客户端节点传送由可执行文件识别的所述应用程序的标识符到所述应用程序服务器。

55.根据权利要求49的系统，其中所述应用程序服务器通过所述连接将文件内容呈现给所述客户端节点。

在提供访问联网内容文件中分配访问控制级的方法和设备

技术领域

[0001] 本发明涉及用于安全访问联网资源的方法和设备，并且具体地，涉及用于在从服务器提供访问联网内容文件中分配访问控制级的方法和设备。

背景技术

[0002] 按照惯例，客户端系统上的用户使用web浏览器和其它基于客户端的应用程序来访问从远端位置取回的内容文件。例如，用户可以使用华盛顿州的雷蒙德(Redmond)的微软公司的INTERNET EXPLORER访问互联网内容，并且然后使用也来自微软公司的WINDOWS EXPLORER来访问桌面产品文件类型，比如已经被下载到本地位置的WORD文档。

[0003] 常规的处理要求下载文件到客户端节点用于观看和处理。然而，从安全性观点看，这种处理存在问题。为了访问客户端上的内容，要求用户两次本地保存该内容到非易失存储器。在下载期间要求第一次保存，并且在上传处理之前编辑之后要求第二次保存。而且，许多用户经常从一个本地目录移动和/或拷贝下载的内容到另一个本地目录(例如，从dir://downloaded_files到dir://my_documents)。这些保存动作的每一个在客户端创建了该文档的一个本地拷贝。客户端设备的极少用户将记得手动删除所述文档的这些本地拷贝，这些拷贝因此保留在客户端设备上。

[0004] 此外，客户端设备的存储器的直接处理对用户来说可能难接近的，比如其中客户端设备位于公用电话亭环境中的情况。在这些情况中，删除本地拷贝的选项对用户来说并不是可以做到的。因为留在客户端上的文档可能是由未被授权的个人通过访问客户端机器所访问的，这提出了显著的安全性问题。另外，较小的设备类型，比如个人数字助理，可能没有足够的资源来允许在设备上使用基于客户端的应用程序。

[0005] 为了试图解决这些顾虑，常规的访问控制方法在准许访问之前可能要求来自客户端的特定认证证书(authentication credential)并且可能拒绝来自不合法位置或设备的访问。然而，常规方法的局限性是通常要求访问控制决定引起要么拒绝要么准许访问资源。在拒绝的情况下，该方法不能提供任何可替换的访问方法。在准许的情况下，该方法可以提供仅完全的和完整的资源公开。通过基于访问控制级分配访问等级来准许访问控制的方法在联网环境中提供对私有资源(proprietary resource)的访问时是所希望的。

[0006] 另外，在保护私有数据不受到不合法客户端节点的访问中，访问权根据诸如客户端设备类型、授权(authorization)证书、以及性能之类的因素来提供访问文件的可替换方法是所希望的。完全拒绝访问权的一种替换方案(比如代表客户端对在安全网络上执行的文件的有限权利)是所希望的。

发明内容

[0007] 本发明涉及通过分配多个访问级之一用于安全访问来自服务器的内容文件以实现增强安全性、证据收集、以及政策应用程序从而提供访问控制的方法和设备。

[0008] 在一个方面中，本发明涉及用于准许访问资源的系统和方法。客户端节点请求访

问资源。收集代理收集关于该客户端节点的信息并且政策机接收所收集的信息。政策机通过响应于政策的应用程序分配多个访问级之一给所接收的信息来做出访问控制决定。

[0009] 在一个实施例中，政策机通过应用政策到所接收的信息做出访问决定。在另一个实施例中，政策机传送该收集代理给客户端节点。

[0010] 在另一个方面中，本发明涉及用于准许访问资源的方法和设备。该设备包括政策机，该政策机包括两个部件。第一部件接收关于客户端节点的信息并且从该信息生成数据组。第二部件接收该数据组，并且基于所接收的数据组将可用于该客户端的资源的枚举(enumeration)提供给第一部件。第一部件将所述资源的枚举呈现给客户端节点。

[0011] 在一个实施例中，第一部件从收集代理接收信息。在一个实施例中，每个部件另外包括数据库。第一部件中的数据库存储条件。第二部件中的数据库存储政策。第一部件应用条件到所接收的信息并且第二部件应用政策到所接收的数据组。在另一个实施例中，第二部件生成可用于客户端节点的资源的子组的枚举。

[0012] 本发明还涉及用于访问网络资源以实现增强的安全性从而减少联网环境中的私有数据的公开的方法和设备。

[0013] 在一个方面中，本发明涉及用于提供文件内容的方法和设备。客户端节点传送文件请求。访问控制服务器接收该请求并且做出访问控制决定。应用程序服务器中心(application server farm)使用与所请求文件的文件类型有关的应用程序将文件内容呈现给客户端节点。

[0014] 在一个实施例中，在做出访问控制决定之前，访问控制服务器收集关于客户端节点的信息。在另一个实施例中，访问控制服务器将可执行文件传送给客户端节点，所述可执行文件包含与文件类型有关的应用程序的标识符和能够将文件内容呈现给客户端节点的应用程序服务器的标识符。在一个实施例中，在将文件内容呈现给客户端节点之前，访问控制服务器识别与文件类型有关的应用程序。在另一个实施例中，在将文件内容呈现给客户端节点之前，应用程序服务器识别与文件类型有关的应用程序。

[0015] 另外，本发明涉及用于访问所转换的文件内容以实现增强的安全性从而提供基于政策的文档控制的方法和设备。

[0016] 在一个方面中，本发明涉及准许访问资源的方法和设备。客户端节点请求访问资源。收集代理收集关于客户端节点的信息。政策机接收所收集的信息并且基于所接收的信息做出访问控制决定。转换服务器从政策机接收文件请求，将文件内容从原始格式转换成第二格式，并且将所转换的文件内容呈现给客户端节点。

[0017] 在一个实施例中，政策机通过应用政策到所接收的信息来做出访问决定。在又一个实施例中，政策机传送收集代理给客户端节点。

[0018] 在另一个方面中，本发明涉及用于准许访问资源的方法和设备。该设备包括政策机，该政策机包括两个部件。第一部件接收关于客户端节点的信息并且从该信息生成数据组。第二部件接收该数据组，并且基于所接收的数据组将可用于该客户端的资源的枚举提供给第一部件。第一部件将所述资源的枚举呈现给客户端节点。

[0019] 在一个实施例中，第一部件从收集代理接收信息。在一个实施例中，每个部件另外包括数据库。第一部件中的数据库存储条件。第二部件中的数据库存储政策。第一部件应用条件到所接收的信息并且第二部件应用政策到所接收的数据组。

附图说明

[0020] 本发明的这些和其它方面将从下面用于示例而并非用于限制本发明的具体描述和附图中变得易于明白，并且其中：

[0021] 图1A是适合于实施本发明的示例性实施例的环境框图；

[0022] 图1B和1C是描绘了用于本发明的计算机的实施例的框图；

[0023] 图1D是计算机网络的实施例的框图，其中该网络提供准许访问网络资源的基于政策的系统；

[0024] 图2是政策机的实施例的更具体的框图；

[0025] 图3是描绘了由政策机基于所接收的关于客户端节点的信息做出访问控制决定所采取的步骤的一个实施例的流程图；

[0026] 图4是计算机网络的实施例的框图，其中网络提供基于政策访问客户端节点的文件内容；

[0027] 图4B是描绘了由应用程序服务器中心(server farm)提供文件内容给客户端节点所采取的步骤的一个实施例的流程图；

[0028] 图5是计算机网络的实施例的框图，其中该网络准许访问所转换的资源内容；

[0029] 图6是描绘了由转换服务器转换所请求的文件内容并且将该转换的内容呈现给客户端节点所采取的步骤的一个实施例的流程图；

[0030] 图7是计算机网络的实施例的框图，其中在该计算机网络中提供了对多个应用程序会话的授权的远端访问；以及

[0031] 图7B是描绘了通过会话服务器使客户端节点与其相关应用程序会话连接所采取的步骤的一个实施例的流程图。

具体实施方式

[0032] 本发明的示例性实施例适用于分布式网络环境，其中远端用户请求访问内容。在讨论本发明的细节之前，讨论某些网络环境将是有帮助的，其中在该网络环境中可以应用本发明的示例性实施例。

[0033] 图1A是适合于实施本发明的示例性实施例的环境框图。客户端节点102包括web浏览器110和应用程序112a，112b…112n。应用程序是处理数据来提供输出并且使用操作系统用于访问系统资源的任何程序。典型应用程序包括：文字处理应用程序，比如由华盛顿州的雷蒙德的微软公司开发的MICROSOFT WORD；电子制表软件程序，比如由微软公司开发的MICROSOFT EXCEL；电子邮件程序，比如由微软公司开发的MICROSOFT OUTLOOK以及由犹他州Provo的Novell公司开发的GROUPWISE；以及产品组，比如由加利福尼亚州Mountain View的Sun Microsystems开发的STAR OFFICE。

[0034] 内容服务器126包括内容文件128并且可以连接到分别保存附加内容文件124和132的数据存储器122和130。本领域的技术人员将意识到，在不背离本发明范围的情况下保存内容文件的其它网络存储设备或文档贮藏库(document repository)也可以被联网到内容服务器126。客户端节点102的用户可以使用web浏览器110从内容服务器126请求内容，来发送请求比如所描绘的超文本传输协议安全(HTTPS)请求115，或者HTTP(超文本传输协

议)、FTP(文件传输协议)请求,或者用于文件共享的操作,SMB(服务器管理块协议)请求。

[0035] 在许多实施例中,内容服务器126、客户端节点102和代理服务器120被提供为由加利福尼亚州Palo Alto的Hewlett-Packard公司或德克萨斯州的Round Rock的戴尔(Dell)公司生产的那种类型的个人计算机或计算机服务器。图1B和1C描绘了在那些实施例中可用作内容服务器126、代理服务器120或客户端节点102的典型计算机100的框图。如图1B和1C中所示,每个计算机100包括中央处理单元102、和主存储器单元104。每个计算机100还可以包括其它任选元件,比如一个或多个输入/输出设备130a-130n(通常涉及使用参考数字130),以及与中央处理单元102进行通信的高速缓存器140。

[0036] 中央处理单元102是响应并且处理从主存储器单元104提取的指令的任何逻辑电路。在许多实施例中,中央处理单元由微处理器单元来提供,所述微处理器单元比如全部由加利福尼亚州的Mountain View的英特尔(Intel)公司生产的8088、80286、80386、80486、奔腾处理器、高能奔腾、奔腾处理器II、Celeron、或Xeon处理器;全部由伊利诺斯州的Schaumburg的摩托罗拉(Motorola)公司生产的68000、68010、68020、68030、68040、PowerPC601、PowerPC604、PowerPC604e、MPC603e、MPC603ei、MPC603ev、MPC603r、MPC603p、MPC740、MPC745、MPC750、MPC755、MPC7400、MPC7410、MPC7441、MPC7445、MPC7447、MPC7450、MPC7451、MPC7455、MPC7457处理器;由加利福尼亚州的Santa Clara的Transmeta公司生产的Crusoe TM5800、Crusoe TM5600、Crusoe TM5500、Crusoe TM5400、Efficeon TM8600、Efficeon TM8300、或Efficeon TM8620处理器;全部由纽约州的White Plains的美国国际商用机器(IBM)公司生产的RS/6000处理器、RS64、RS64II、P2SC、POWER3、RS64III、POWER3-II、RS64IV、POWER4、POWER4+、POWER5或POWER6处理器;或由加利福尼亚州的Sunnyvale的AMD(Adcanced Micro Devices)公司生产的AMD Opteron、AMD Athalon64FX、AMD Athalon、或AMD Duron处理器。

[0037] 主存储器单元104可以是能够存储数据并且允许微处理器102直接访问任意存储位置的一个或多个存储器芯片,比如静态随机访问存储器(SRAM)、或突发式SRAM或同步突发式SRAM(BSRAM)、动态随访访问存储器(DRAM)、快速页面模式DRAM(FPM DRAM)、增强DRAM(EDRAM)、可扩展数据输出RAM(EDO RAM)、可扩展数据输出DRAM(EDO DRAM)、突发可扩展数据输出DRAM(BEDO DRAM)、增强DRAM(EDRAM)、同步DRAM(SDRAM)、JEDEC SRAM、PC100SDRAM、双数据速率SDRAM(DDR SDRAM)、增强SDRAM(ESDRAM)、同步链路DRAM(SLDRAM)、直接Rambus DRAM(DRDRAM)、或铁电RAM(FRAM)。

[0038] 在图1B中所示的实施例中,处理器102通过系统总线120(下面将更具体地加以描述的)与主存储器104进行通信。图1C描绘了计算机系统100的实施例,其中处理器通过存储器端口直接与主存储器104进行通信。例如,在图1C中,主存储器104可以是DRDRAM。

[0039] 图1B和图1C描绘了其中主处理器102通过有时称作“后方”总线的第二总线直接与高速缓存器140进行通信的实施例。在其它实施例中,主处理器102使用系统总线120与高速缓存器140进行通信。高速缓存器140典型地具有比主存储器104更快的响应时间并且典型地由SRAM、BSRAM、或EDRAM提供。

[0040] 在图1B中示出的实施例中,处理器102通过本地系统总线120与各种I/O设备130进行通信。各种总线可以用于连接中央处理单元102到I/O设备130,所述总线包括VESA VL总线、ISA总线、EISA总线、微通道结构(MCA)总线、PCI总线、PCI-X总线、PCI－Express总线、或

NuBus总线。对于其中所述I/O设备为视频显示器的实施例，处理器102可以使用加速图形接口(AGP)来与显示器通信。图1C描绘了计算机系统100的实施例，其中主处理器102通过HyperTransport(超高速传输)、快速I/O(Rapid I/O)、或InfiniBand(无限带宽)直接与I/O设备130b进行通信。图1C还描绘了其中混合了本地总线和直接通信的实施例：处理器102使用本地互连总线与I/O设备130a通信同时与I/O设备130b直接进行通信。

[0041] 多种I/O设备130可以呈现在计算机系统100中。输入设备包括键盘、鼠标、跟踪板、跟踪球、麦克风、以及写字板。输出设备包括视频显示器、扬声器、喷墨打印机、激光打印机、以及染料升华打印机(dye-sublimation printer)。I/O设备还可以提供用于计算机系统100的大容量存储器，比如硬盘驱动器、用于容纳软盘比如3.5英寸、5.25英寸磁盘或ZIP磁盘的软盘驱动器、CD-ROM驱动器、CD-R/RW驱动器、DVD-ROM驱动器、各种格式的磁带驱动器、以及USB存储器设备比如由加利福尼亚的洛杉矶的Twintech Industry公司生产的设备的USB闪速驱动线。

[0042] 在另一个实施例中，I/O设备130可以是系统总线120和外部通信总线之间的电桥(bridge)，外部通信总线比如是USB总线、Apple Desktop Bus(苹果桌面总线)、RS-232串行连接、SCSI总线、火线(FireWire)总线、火线800总线、以太网总线、AppleTalk总线、吉比特以太网总线、异步传输模式总线、HIPPI总线、超HIPPI总线、SerialPlus总线、SCI/LAMP总线、光纤通道(FibreChannel)总线、或者串行连接小型计算机系统接口总线。

[0043] 图1B和图1C中描绘的那种通用桌面计算机通常在操作系统的控制下工作，所述操作系统控制任务调度并且访问系统资源。其中，典型操作系统包括：由华盛顿州的雷蒙德的微软公司开发的MICROSOFT WINDOWS；由加利福尼亚州的库珀蒂诺(Cupertino)的苹果计算机(Apple Computer)公司开发的MacOS；由纽约州的Armonk的国际商用机器(IBM)公司开发的OS/2；以及犹他州的盐湖城(Salt Lake City)的Caldera公司供销的免费获得的操作系统Linux。

[0044] 客户端节点102可以是任何个人计算机(例如，286、386、486、奔腾、奔腾II、Macintosh计算机)、基于视窗的终端、网络计算机、无线设备、信息设备、RISC Power PC、X设备、工作站、微型计算机、主机计算机、个人数字助理、或具有基于视窗的桌面并且具有足够的永久存储器用于执行小型显示器显示节目的其它计算设备。显示器显示节目使用通过通信通道发送给它的命令和数据来呈现图形显示。所述客户端节点102支持的面向视窗的平台可以包括但不限于WINDOWS3.x、WINDOWS95、WINDOWS98、WINDOWS NT3.51、WINDOWS NT4.0、WINDOWS2000、WINDOWS CE、MAC/OS、Java以及UNIX。客户端节点102可以包括可视显示器设备(例如，计算机监视器)、数据输入设备(例如，键盘)、用于存储下载的应用程序的永久或易失存储器(例如，计算机存储器)、处理器、以及鼠标。小型显示器显示节目的执行允许客户端节点102参与分布式计算机系统模型(即，基于服务器的计算模型)。

[0045] 对于其中客户端节点102为移动设备的实施例，所述设备可以是JAVA使能的蜂窝电话，比如全部由伊利诺斯州的Schaumburg的摩托罗拉(Motorola)公司生产的i50sx、i55sr、i58sr、i85s、i88s、i90c、i95cl、或iml1000；由日本京都的Kyocera生产的6035或7135；或者韩国汉城的三星电子有限公司生产的i300或i330。在其中客户端节点102为移动的其它实施例中，它可以是在PalmOS操作系统控制下工作的个人数字助理(PDA)，比如全部由加利福尼亚州的Milpitas的palmOne公司生产的Tungsten W、VII、VIIx、i705。在另外的

实施例中，客户端节点102可以是在PocketPC操作系统控制下工作的个人数字助理(PDA)，比如全部由加利福尼亚州的Palo Alto的Hewlett-Packard公司生产iPAQ4155、iPAQ5555、iPAQ1945、iPAQ2215、以及iPAQ4255；由加利福尼亚州的Walnut的ViewSonic公司生产的ViewSonic V36；或者由纽约州的纽约的东芝美国公司生产的东芝PocketPC e405。在又一个实施例中，客户端节点是组合PDA/电话设备，比如全部由加利福尼亚州的Milpitas的palmOne公司生产的Treo180、Treo270或Treo600。在又一个实施例中，客户端节点102为在PocketPC操作系统控制下工作的蜂窝电话，比如由摩托罗拉公司生产的MPx200。

[0046] 现在参照图1D，描绘了根据本发明构建的计算机网络100的一个实施例，其包括客户端节点102、收集代理104、政策机106、政策数据库108、应用程序服务器中心114、以及应用程序服务器116。尽管在图1D所示的实施例中仅描绘了一个客户端节点102、收集代理104、政策机106、应用程序服务器中心114、以及应用程序服务器116，应当理解本系统可以提供这些部件中任意一种或每一种的多个。例如，在一个实施例中，系统100包括多个逻辑分组的应用程序服务器116，其中的每一个可用于代表所述客户端节点102执行应用程序。在这些实施例中，该逻辑组服务器可以称作“服务器中心”。在这些实施例的某些实施例中，服务器可以在地理上被分散。

[0047] 概言之，当客户端节点102传送请求110到政策机106用于访问资源时，收集代理104与客户端节点102进行通信，取回关于客户端节点102的信息，并且传送客户端节点信息112到政策机106。政策机106通过将来自政策数据库108的政策应用到所接收的信息112做出访问控制决定。

[0048] 更具体地，客户端节点102传送用于资源的请求110到政策机106。在某些实施例中，客户端节点102通过网络连接传送请求110。网络可以是局域网(LAN)、城域网(MAN)、或者广域网(WAN)比如互联网。客户端节点102和政策机106可以通过多种连接而连接到网络，所述连接包括标准电话线、LAN或WAN链路(例如，T1、T3、56kb、X.25)、宽带连接(ISDN、帧中继、ATM)、以及无线连接。客户端节点102和政策机106之间的连接可以使用多种数据链路层通信协议(例如，TCP/IP、IPX、SPX、NetBIOS、NetBEUI、SMB、Ethernet(以太网)、ARCNET、光纤分布式数据接口(FDDI)、RS232、IEEE802.11、IEEE802.11a、IEEE802.11b、IEEE802.11g以及直接异步连接)。

[0049] 一旦接收到请求，政策机106通过收集代理104发起信息收集。收集代理104收集关于客户端节点102的信息并且将信息112传送给政策机106。

[0050] 在一些实施例中，收集代理104收集并且通过网络连接传送信息112。在一些实施例中，收集代理104包括字节码，比如以字节码编程语言JAVA编写的应用程序。在一些实施例中，收集代理104包括至少一个脚本。在那些实施例中，收集代理104通过在客户端节点102上运行至少一个脚本来收集信息。在一些实施例中，收集代理包括在客户端节点102上的Active X控件。Active X控件是一种实现一组接口的专用COM(组件对象模型)对象，该接口使得其能够看起来和做起来像一种控件。

[0051] 在一些实施例中，收集代理104在客户端节点上执行。在其它实施例中，收集代理104位于政策机106上。在又一些实施例中，收集代理104位于服务器上。在其它实施例中，政策机106位于该服务器上。在这些实施例的某些实施例中，收集代理104位于政策机106和该服务器上。

[0052] 在一个实施例中，政策机106传送收集代理104给客户端节点102。在一个实施例中，在收集代理104已经传送信息112给政策机106之后，政策机106需要收集代理104的第二次执行。在这个实施例中，政策机106可以具有不足信息112来判定客户端节点102是否满足特定条件。在其它实施例中，政策机106响应于所接收的信息112要求收集代理104的多次执行。

[0053] 在一些实施例中，政策机106传送指令给收集代理104确定收集代理104收集的信息类型。在那些实施例中，系统管理员可以配置从政策机106传送到收集代理104的指令。这对所收集的信息类型提供了更大控制。由于对于所收集的信息的类型提供了更大控制，这还扩展了政策机106可以做出的访问控制决定的类型。收集代理104收集信息112，该信息包括但不限于客户端节点的机器ID、操作系统类型、操作系统补丁的存在、被安装的网卡的MAC地址、客户端设备上的数字水印、有效目录(active directory)中的从属关系、病毒扫描软件(virus scanner)的存在、个人防火墙的存在、HTTP报头、浏览器类型、设备类型、网络连接信息、以及授权证书。

[0054] 在一些实施例中，设备类型是个人数字助理。在其它实施例中，设备类型是蜂窝电话。在其它实施例中，设备类型是膝上型计算机。在其它实施例中，设备类型是桌上型计算机。在其它实施例中，设备类型是互联网公用电话亭(Internet kiosk)。

[0055] 在一些实施例中，数字水印包括数据嵌入。在一些实施例中，水印包括插入文件中的数据模式以提供关于该文件的源信息。在其它实施例中，水印包括数据散列文件以提供篡改检测。在其它实施例中，水印提供关于所述文件的版权信息。

[0056] 在一些实施例中，网络连接信息与带宽能力有关。在其它实施例中，网络连接信息与互联网协议地址有关。在又一些实施例中，网络连接信息包含互联网协议地址。在一个实施例中，网络连接信息包括网络区域(network zone)，该网络区域识别登录上网代理，客户端节点提供认证证书给该登录上网代理。

[0057] 在一些实施例中，授权证书包括多种类型的认证信息，包括但不限于用户名、客户端名、客户端地址、口令、PIN、语音采样、一次性口令、生统统计数据(biometric data)、数字证书、标签等等及其组合。在接收到所收集的信息112之后，政策机106基于所接收的信息112做出访问控制决定。

[0058] 现在参照图2，它是政策机200的一个实施例的框图，包括第一部件202和第二部件210，其中第一部件202包括条件数据库204和登录上网代理206，第二部件210包括政策数据库212。第一部件202将来自条件数据库204的条件应用到所接收的关于客户端节点102的信息并且判定所接收的信息是否满足条件。

[0059] 在一些实施例中，第一部件202和第二部件210逻辑上独立但物理上不独立。在一些实施例中，第一部件202和第二部件210逻辑和物理上独立。在一些实施例中，条件数据库204位于第一部件202上。在其它实施例中，条件数据库204位于第二部件210上。

[0060] 在一些实施例中，条件可以要求客户端节点102执行特定操作系统来满足该条件。在一些实施例中，条件可以要求客户端节点102执行特定操作系统补丁以满足该条件。在又一些实施例中，条件可以要求客户端节点102提供用于每个被安装的网卡的MAC地址以满足该条件。在一些实施例中，条件可以要求客户端节点102表明在特定有效目录中的从属关系以满足该条件。在另外的实施例中，条件可以要求客户端节点102执行病毒扫描软件以满足

条件。在其它实施例中，条件可以要求客户端节点102执行个人防火墙以满足该条件。在一些实施例中，条件可以要求客户端节点102包括特定设备类型以满足该条件。在其它实施例中，条件可以要求客户端节点102建立特定类型的网络连接以满足该条件。

[0061] 如果所接收的信息满足条件，那么第一部件202在数据组208中为那个条件存储标识符。在一个实施例中，如果信息使得条件为真，那么所接收的信息满足条件。例如，条件可以要求安装特定操作系统。如果客户端节点102具有那个操作系统，那么该条件为真并且满足。在另外的实施例中，如果信息使得条件为假，则所接收的信息满足条件。例如，条件可以针对spyware(间谍软件)是否存在客户端节点102上。如果客户端节点102不包含间谍软件，则条件为假并且满足。

[0062] 在一些实施例中，登录上网代理206位于政策机200之外。在其它实施例中，登录上网代理206位于政策机200上。在一个实施例中，第一部件202包括登录上网代理206，该登录上网代理206发起关于客户端节点102的信息收集。在一些实施例中，登录上网代理206进一步包括数据存储器。在这些实施例中，数据存储器包括收集代理可以收集信息的条件。这个数据存储器不同于条件DB204。

[0063] 在一些实施例中，登录上网代理206通过执行收集代理104发起信息收集。在其它实施例中，登录上网代理206通过传送收集代理104给客户端节点102发起信息收集用于在客户端节点102上执行。在又一些实施例中，登录上网代理206在接收信息112之后发起另外的信息收集。在一个实施例中，登录上网代理206也接收信息112。在这个实施例中，登录上网代理206基于所接收的信息112生成数据组208。在一些实施例中，登录上网代理206通过将来自数据库204的条件应用到从收集代理104接收的信息来生成数据组208。

[0064] 在另外的实施例中，第一部件202包括多个登录上网代理206。在这个实施例中，所述多个登录上网代理206中的至少一个位于每个网络域上，客户端节点102可以从所述每个网络域传送资源请求。在这个实施例中，客户端节点102传送资源请求给特定登录上网代理206。在一些实施例中，登录上网代理206将客户端节点102从其访问登录上网代理206的所述网络域传送给政策机200。在一个实施例中，客户端节点102从其访问登录上网代理206的网络域被称作客户端节点102的网络区域。

[0065] 条件数据库204存储第一部件202应用到所接收信息的条件。政策数据库212存储第二部件210应用到所接收数据组的政策。在一些实施例中，条件数据库204和政策数据库212在ODBC相容数据库中存储数据。例如，条件数据库204和政策数据库212可以被提供为由加利福尼亚州的Redwood Shores的Oracle公司开发的ORACLE数据库。在其它实施例中，条件数据库204和政策数据库212可以是华盛顿州的雷蒙德的微软公司开发的Microsoft ACCESS数据库或Microsoft SQL服务器数据库。

[0066] 在第一部件202将所接收的信息应用到条件数据库204中的每个条件之后，第一部件传送数据组208到第二部件210。在一个实施例中，第一部件202仅传送数据组208到第二部件210。因此，在这个实施例中，第二部件210不接收信息112，仅接收满足条件的标识符。第二部件210接收数据组208并且基于数据组208中所识别的条件通过应用来自政策数据库212的政策做出访问控制决定。

[0067] 在一个实施例中，政策数据库212存储应用到所接收的信息112的政策。在一个实施例中，存储在政策数据库212中的政策至少部分地由系统管理员指定。在另外的实施例

中，用户指定存储在政策数据库212中的至少一些政策。用户指定的一个或多个政策被存储为优先选择。政策数据库212可以被存储在易失或非易失存储器中或者例如通过多个服务器分配。

[0068] 在一个实施例中，只有当满足一个或多个条件，政策才允许访问资源。在另外的实施例中，政策允许访问资源但是禁止传送资源到客户端节点102。存储在政策数据库212中的政策之一可能要求或者禁止自动连接到断开的应用程序会话。又一政策可能做出发生在客户端节点102上的连接，该连接请求在安全网络中进行访问。另一政策可能要求或者禁止自动连接到当前被连接到不同客户端节点102的有效应用程序会话。另一政策可能仅允许在接收到用户准许之后连接到应用程序会话。另一政策可能仅在断开之后预定时间允许连接。又一个政策可能仅允许连接到包括特定应用程序的应用程序会话。一种政策可能允许仅仅观看请求文件的转换内容。一种政策可能允许仅仅观看请求文件的HTML版本。在一些实施例中，提供访问资源同时防止文件下载到客户端节点102。这可能以多种方式来完成，包括：转换文件内容为仅阅读器格式、转换文件内容为HTML，用于使用web浏览器观看、使用相关的文件类型来使用服务器中心的服务器拥有的应用程序，而不是使用客户端节点102拥有的应用程序打开文件、或者通过使用在美国专利申请序列号10/931405中描述的那种系统，该申请的内容在此作为参考被结合进来。

[0069] 在上面的一些实施例中，该方法和设备提供私有信息的文档保护。在这些实施例中，客户端节点不能访问联网资源除非政策机106准许客户端节点102允许访问资源。在这些实施例之一中，政策机106为单个外露的网络元件，用来保证客户端节点102必须访问政策机106以便访问联网资源。在这些实施例的另一个实施例中，用于在政策机106之后访问联网资源的URL被重新写入来防止客户端节点102的直接访问。在上面其它实施例中，所述方法和设备增强客户端节点访问资源的能力，该资源用别的方式是不可访问的。在上面的一些实施例中，所述方法和设备提供私有信息的保护和增强的客户端节点能力。

[0070] 现在参照图3，流程图描绘了由政策机106基于所接收的关于客户端节点102的信息做出访问控制决定所采取的步骤的一个实施例。一旦接收到所收集的关于客户端节点102的信息(步骤350)，政策机106基于所述信息生成数据组(步骤352)。在一些实施例中，政策机106从收集代理104请求关于客户端节点102的另外信息。在这些实施例中，政策机106要求在客户端节点102上不止一次执行收集代理104。在那些实施例中，政策机106在接收到附加的请求信息之后生成数据组108。在这些实施例中，政策机106可以具有不足的信息112来判定客户端节点102是否满足特定条件。在这些实施例的其它实施例中，条件可以是不确定的。在其中条件是不确定的一些实施例中，收集代理不能收集满足该条件所要求的信息。

[0071] 数据组208包含由所接收信息112所满足的每个条件的标识符。接着，政策机106将政策应用到数据组208中的每个所识别的条件。那个应用程序产生客户端节点102可以访问的资源的枚举(步骤354)。在一个实施例中，资源包括私有数据。在一些实施例中，资源包括web网页。在其它实施例中，资源包括文字处理文档。在又一些实施例中，资源包括电子制表软件。在一些实施例中，所述枚举包括仅客户端节点102可以访问的资源的子组。政策机106然后将所述枚举呈现给客户端节点102。在一些实施例中，政策机106创建用于将所述枚举呈现给客户端节点的超文本链接标示语言(HTML)文档。

[0072] 现在参照图4，描绘了根据本发明构建的计算机网络400的一个实施例，其包括客

户端节点402、收集代理404、访问控制服务器406、政策数据库408、应用程序服务器中心414、第一应用程序服务器416、应用程序数据库418、第二应用程序服务器420、以及第二应用程序数据库422。在一些实施例中，存在将客户端节点402所位于的网络与访问控制服务器406和应用程序服务器中心414所位于的网络分隔的网络边界。

[0073] 概言之，当客户端节点402传送访问资源的请求410给访问控制服务器406时，收集代理404与客户端节点402进行通信，取回关于客户端节点402的信息，并且传送客户端节点信息412至访问控制服务器406。在一个实施例中，在政策机106向客户端节点402呈现可用资源的枚举之后，客户端节点402传送请求410。访问控制服务器406通过将来自政策数据库408的政策应用到所接收的信息412做出访问控制决定。最后，访问控制服务器406传送文件类型给应用程序服务器中心414用于将文件内容呈现给客户端节点402。省略了计算机网络400的附加部件并且其将在图4B中进一步加以描述。

[0074] 现在参照图4B，流程图描绘了访问控制服务器406和应用程序服务器中心414提供文件内容给客户端节点402所采取的步骤的一个实施例。应用程序服务器中心414的一部分是应用程序服务器416。

[0075] 在一个实施例中，一旦访问控制服务器406决定准许客户端节点402访问所请求的文件，则访问控制服务器406确定所请求的文件的文件类型(步骤452)。在其它实施例中，应用程序服务器416确定所请求的文件的文件类型。在又一些实施例中，除了应用程序服务器416或者访问控制服务器406之外的服务器。在一些实施例中，确定文件类型的服务器必须首先取回所请求的文件。在那些实施例的一些实施例中，文件位于网络边界424的与确定文件类型的服务器同一侧。在那些实施例的其它实施例中，文件位于网络边界424的与客户端节点402同一侧。在这些实施例中，所述方法和设备增强了客户端节点访问资源的能力，该资源用别的方式是不可访问的，但是它们不提供私有信息的文档保护。

[0076] 在一些实施例中，网络边界424物理上分割至少两个网络。在其它实施例中，网络边界424逻辑上分割至少两个网络。在一个实施例中，网络边界424是防火墙。

[0077] 在一个实施例中，文件扩展名是文件类型并且确定文件类型的服务器通过从文件中提取文件扩展名来做到这一点。在另一个实施例中，资源分支(resource fork)是文件类型。在确定文件类型之后，确定文件类型的服务器传送文件类型给应用程序服务器中心414用于取回和呈现给客户端节点402(步骤454)。

[0078] 应用程序服务器416从访问控制服务器406接收文件类型(步骤456)。在一些实施例中，应用程序服务器416识别与那个文件类型有关的应用程序。在其它实施例中，访问控制服务器406识别与那个文件类型有关的应用程序。在又一些其它实施例中，除了访问控制服务器406或应用程序服务器416之外的服务器识别与那个文件类型有关的应用程序。

[0079] 在一个实施例中，识别与文件类型有关的应用程序的服务器查询应用程序数据库418来取回用于应用程序的标识符。在一些实施例中，应用程序数据库418是登记文件。在其中应用程序服务器416或单独服务器基于文件类型识别应用程序类型的实施例中，识别服务器于是传送应用程序的所述标识符给访问控制服务器406。在一些实施例中，识别服务器通过网络连接传送标识符给访问控制服务器406。

[0080] 在一些实施例中，访问控制服务器406或单独服务器都不需要传送文件类型给应用程序服务器416，以确定相关应用程序的标识符。在这些实施例之一中，应用程序服务器

416传送所拥有的应用程序列表和与那些应用程序有关的文件类型给访问控制服务器406。在这些实施例中，访问控制服务器406从所传送的列表中取回与文件类型有关的应用程序的标识符。

[0081] 当访问控制服务器406接收应用程序的标识符时，访问控制服务器406创建并且传送可执行文件给客户端节点402(步骤458)。在一些实施例中，可执行文件包含应用程序的标识符。在一些实施例中，可执行文件包含将文件内容呈现给客户端节点402的应用程序服务器中心414中的应用程序服务器的标识符。在一些实施例中，使用文件类型识别应用程序的同一应用程序服务器416将文件内容呈现给客户端节点402。在其它实施例中，第二应用程序服务器420将文件内容呈现给客户端节点402。在一个实施例中，可执行文件包含应用程序的标识符和将文件内容呈现给客户端节点402的应用程序服务器中心414中的应用程序服务器的标识符。在一些实施例中，可执行文件使得客户端节点402能够使用表示层协议，比如来自佛罗里达的Fort Lauderdale的Citrix Systems公司的独立计算结构(ICA)协议与所识别的服务器连接。在其它实施例中，可执行文件使得客户端节点402能够使用微软公司开发的远端桌面协议(RDP)，与所识别的服务器连接。在其它实施例中，表示层协议被封装在较高层的协议中。

[0082] 客户端节点402从访问控制服务器406接收可执行文件。客户端节点402连接到在可执行文件中识别的应用程序服务器416(步骤460)。在一个实施例中，客户端节点402使用ICA协议连接到所识别的应用程序服务器416。在另一个实施例中，客户端节点402使用RDP连接到所识别的应用程序服务器416。

[0083] 应用程序服务器416选择呈现文件内容的格式(步骤464)。在其它实施例中，访问控制服务器406识别用于呈现文件内容的格式。在那些实施例中，访问控制服务器406可应用政策来识别可用格式。在一些实施例中，应用程序服务器416基于所接收的关于客户端节点402的信息选择格式。在其它实施例中，应用程序服务器416通过将政策应用到所接收的信息来选择格式。

[0084] 应用程序服务器416接受客户端节点402连接并且取回所请求的文件(步骤466)。在一个实施例中，应用服务器416从web服务器取回文件。在另一个实施例中，应用程序服务器416从文件服务器取回文件。在又一个实施例中，所取回的文件是电子邮件的附件。在这个实施例中，应用程序服务器416从电子邮件服务器中取回文件。在一些实施例中，邮件服务器是Lotus邮件服务器。在其它实施例中，邮件服务器是OutLook邮件服务器或者OutLook Web Access邮件服务器。

[0085] 应用程序服务器416通过连接将文件内容呈现给客户端节点402(步骤468)。在一个实施例中，所呈现的文件内容包含电子邮件附件。

[0086] 参照图5，描绘了根据本发明构建的计算机网络500的一个实施例，该计算机网络包括客户端节点502，收集代理504，政策机506，第一部件508，第二部件512，条件数据库510，政策数据库512，转换服务器516，和存储元件518。概言之，当客户端节点502从政策机506传送用于访问资源的请求522时，收集代理504与客户端节点502进行通信，取回关于客户端节点502的信息，并且传送客户端节点信息512至政策机506。政策机506做出访问控制决定，如上面图3中所讨论的。一旦政策机506决定准许客户端节点502访问所请求的文件，则政策机506传送该请求至转换服务器516用于转换和呈现给客户端节点502。

[0087] 更具体地，政策机506从客户端节点502接收用于所转换的文件内容的请求。在一个实施例中，政策机506识别能够将所转换的文件内容呈现给客户端节点502的转换服务器516。在一些实施例中，转换服务器516能够呈现转换的文件内容，因为它包含之前转换的内容的拷贝。在其它实施例中，转换服务器516能够呈现转换的文件内容，因为它当前有能力转换文件内容。

[0088] 在一个实施例中，政策机506通过查询一个存储元件518以决定是否转换服务器516之前转换了文件内容来识别转换服务器516。在那个实施例中，政策机506传送由存储元件518识别的转换服务器518的标识符给客户端节点502。在其它实施例中，没有任何转换服务器516之前转换内容。在那些实施例中，政策机而是识别当前能够转换文件内容的转换服务器516并且传送客户端节点502的请求至那个转换服务器516。

[0089] 在其它实施例中，除了政策机506之外的服务器识别能够将所转换的文件内容呈现给客户端的转换服务器516。在这些实施例的一些实施例中，同一服务器还向转换服务器516传送将文件呈现给客户端的请求。在这些实施例的一些实施例中，识别有能力的转换服务器516的同一服务器通过代理服务器路由并且传送所述请求给转换服务器516。

[0090] 在一个实施例中，转换服务器516接收来自政策机506的请求用于转换所请求文件的内容并且呈现给客户端节点502。在另一实施例中，转换服务器516接收来自除了政策机506之外的服务器的请求。转换服务器516取回文件并且将内容从原始格式转换成第二格式。转换服务器516然后接受来自客户端节点502的连接并且呈现所转换的文件内容，如果所述内容先前没有转换的话则转换所述内容。最后，转换服务器516将转换文件内容的服务器的标识符和文件的标识符写入存储元件518。

[0091] 现在参照图6，流程图描绘了由转换服务器516转换所请求的文件内容并且将该转换的内容呈现给客户端节点502所采取的步骤的一个实施例。

[0092] 转换服务器516接收所请求文件的内容的转换请求并且呈现给客户端节点502(步骤600)。在一个实施例中，转换服务器516通过网络连接接收这个请求。

[0093] 转换服务器516将所请求的文件内容从原始格式转换为第二格式(步骤602)。在一个实施例中，转换服务器516使用规则表示将文件内容从原始格式转换为第二格式用于呈现在客户端上。在另一实施例中，转换服务器516将文件内容从原始格式转换成第二格式，其包含格式转换工具。在另一实施例中，转换服务器516将文件内容从原始格式转换成HTML。在另一实施例中，转换服务器516将文件内容从原始格式转换成第二格式，其中第二格式使得能够在个人数字助理上呈现。在另一实施例中，转换服务器516将文件内容从原始格式转换成第二格式，其中第二格式使得能够在蜂窝电话上呈现。在另一实施例中，转换服务器516将文件内容从原始格式转换为第二格式，其中第二格式使得能够在膝上型计算机上呈现。在另一实施例中，转换服务器516将文件内容从原始格式转换为第二格式，其中第二格式使得能够在互联网公用电话亭上呈现。

[0094] 转换服务器516将关于所述转换的识别信息写入存储元件518(步骤604)。在一个实施例中，识别信息包括转换服务器516的标识符以及所转换的文件的标识符。在一些实施例中，识别信息包括临时文件，该临时文件包含所转换的文件内容。在那些实施例中，存储元件518用作所转换的文件内容的全局高速缓存器。

[0095] 在政策机506识别能够呈现用于客户端节点502的所转换的文件内容的转换服务

器516之后，政策服务器506传送转换服务器516的标识符给客户端节点502。客户端节点502接收标识符并且连接到转换服务器516。转换服务器516接受所述连接并且通过该连接将所请求文件的转换内容呈现给客户端节点502(步骤606)。在一个实施例中，转换服务器516在呈现给客户端节点502之后保留所请求文件的转换内容。

[0096] 参照图7，描绘了根据本发明构建的计算机网络700的一个实施例，其包括第一客户端节点702、收集代理704、政策机706、政策数据库708、条件数据库710、第二客户端节点716、会话服务器720、所存储的应用程序数据库722、应用程序服务器中心724、第一应用程序服务器726、第一数据库728、第二应用程序服务器730、以及第二数据库732。概言之，当第一客户端节点702传送访问资源的请求712到访问控制服务器706时，收集代理704与客户端节点702进行通信，取回关于客户端节点702的信息，并且传送客户端节点信息714给政策机706。政策机706做出访问控制决定，如上面图3中所讨论的。最后，会话服务器720在客户端节点702和与客户端节点702有关的多个应用程序会话之间建立连接。计算机网络700的附加部件被省略并且其将在图7B中进一步加以描述。

[0097] 现在参照图7B，流程图描绘了由会话服务器720使客户端节点702与其相关应用程序会话连接所采取的步骤的一个实施例。会话服务器720从政策机706接收关于客户端节点702的包含政策机706做出的访问控制决定的信息。在一个实施例中，该信息还包括客户端节点信息714。

[0098] 在一些实施例中，政策机706识别已经与客户端节点702有关的多个应用程序会话。在其它实施例中，会话服务器720识别与客户端节点702有关的所存储的应用程序会话。在这些实施例的一些实施例中，一接收到来自政策机706的信息，会话服务器720自动识别所存储的应用程序会话。在一个实施例中，所存储的应用程序数据库722位于会话服务器720上。在另一实施例中，所存储的应用程序数据库722位于政策机706上。

[0099] 所存储的应用程序数据库722包含与执行应用程序会话的应用程序服务器中心724中的多个服务器有关的数据。在一些实施例中，识别与客户端节点702有关的应用程序会话要求查阅与执行应用程序会话的一个或多个服务器有关的存储数据。在这些实施例的一些实施例中，会话存储器720查阅与执行应用程序会话的一个或多个服务器有关的存储数据。在这些实施例的其它实施例中，政策机706查阅与执行应用程序会话的一个或多个服务器有关的存储数据。在一些实施例中，第一应用程序会话运行在第一应用程序服务器726上并且第二应用程序会话运行在第二应用程序服务器730上。在其它实施例中，所有应用程序会话运行在应用程序服务器中心724中的单个应用程序服务器上。

[0100] 会话服务器720包括与由用户发起的应用程序会话有关的信息。会话服务器可以被存储在易失或非易失存储器中，或者例如通过多个服务器分配。表格7-1示出了包括在所示例性会话服务器720的一部分中的数据。

[0101] 表格7-1

[0102]

应用程序会话	应用程序会话1	应用程序会话2	应用程序会话3
用户ID	用户1	用户2	用户1
客户端ID	第一客户端		第一客户端
客户端地址	172.16.0.50		172.16.0.50

状态	有效	断开	有效
应用程序	文字处理器	数据库	电子制表软件
处理序号	1	3	2
服务器	服务器A	服务器A	服务器B
服务器地址	172.16.2.55	172.16.2.55	172.16.2.56

[0103] 表格7-1中的示例性会话服务器720包括使每个应用程序会话与发起应用程序会话的用户相关联的数据，客户端计算机702或716的标识，如果有的话，当前用户从其被连接到服务器726、以及那个客户端计算机702a或716的IP地址。所示例的会话服务器720还包括每个应用程序会话的状态。应用程序会话状态可以例如为“有效”（指用户被连接到应用程序会话）或者“断开”（指用户没有连接到应用程序会话）。在可替换的实施例中，应用程序会话状态还可以被设置为“执行-断开”（指用户已经从所述应用程序会话断开，但是应用程序会话中的应用程序仍旧执行），或者“停止-断开”（指用户断开并且应用程序会话中的应用程序没有执行，但是它们的工作状态在断开之前立即被保存）。会话服务器720进一步存储表示在每个应用程序会话中执行的应用程序116和表示在服务器上每个应用程序处理的数据的信息。在其中服务器726为服务器中心724的一部分的实施例中，会话服务器720至少为动态存储器的一部分，并且还包括表格1的最后两行中的数据，该数据表示每个应用程序正在服务器中心中的哪个服务器上执行，以及那个服务器的IP地址。在可替换的实施例中，会话服务器720包括在每个应用程序会话中的每个应用程序的状态指示符。

[0104] 例如，在表格7-1的例子中，存在三个应用程序会话，即应用程序会话1、应用程序会话2、和应用程序会话3。应用程序会话1与用户1相关联，该用户当前使用终端1。终端1的IP地址为152.16.2.50。应用程序会话1的状态为有效，并且在应用程序会话1中，正在执行文字处理程序。文字处理程序在服务器A上执行，作为处理序号1。服务器A的IP地址是152.16.2.55。表格1中的应用程序会话2是断开的应用程序会话118的例子。应用程序会话2与用户2相关联，但是应用程序会话2没有连接到客户计算机702a或716。应用程序会话2包括在服务器A上执行的数据库程序，服务器A的IP地址为152.16.2.55，处理序号为3。应用程序会话3是用户如何与在不同服务器726上工作的应用程序会话交互的例子。应用程序会话3与应用程序会话1一样也与用户1相关联。应用程序会话3包括在服务器B上执行的电子制表软件程序，服务器B的IP地址是152.16.2.56，处理序号为2，而包括在应用程序会话1中的应用程序会话在服务器A上执行。

[0105] 在一个实施例中，会话服务器720被配置来接收断开请求来断开与客户端节点702有关的应用程序会话并且响应于所述请求这么做来断开应用程序会话。会话服务器720在从应用程序会话断开客户端节点702之后继续执行应用程序会话。在这个实施例中，会话服务器720访问所存储的应用程序数据库722并且更新与每个断开应用程序会话有关的数据记录，这样该记录表示与客户端节点702有关的应用程序会话是断开的。

[0106] 由不完善网络连接和用户自己不能终止它们的应用程序会话引起的应用程序会话的无意识终止可以给用户带来麻烦。本发明的一个实施例通过区分断开（其被当作用户没有完成与应用程序会话一起工作来处理）与终止（其被假设为有意结束应用程序会话）并且通过将应用程序会话与相对于客户端节点的用户相关，限制这些麻烦。当用户使用工作在应用程序会话中的应用程序结束时，用户可以终止应用程序会话。终止通常包括表示服

务器应当不再保持应用程序会话的用户肯定输入。这样的肯定用户输入可以包括从菜单选择“退出”选项，点击图标等等。响应于接收终止请求的会话服务器720，暂停那个应用程序会话中的应用程序会话和任何应用程序的执行。在一个实施例中，与应用程序会话有关的数据也从所存储的应用程序数据库722中移除。

[0107] 另一方面，不管是有意还是无意的断开，不会引起应用程序会话的终止。由于工作在应用程序会话中的一个或多个应用程序在服务器720上执行，到第一客户端节点702的连接通常不必继续执行应用程序，并且在一个实施例中，应用程序可以继续执行同时等待用户连接。在可替换的实施例中，一旦断开用户，会话服务器720停止工作在应用程序会话中的应用程序的执行。即，会话服务器720停止应用程序的进一步执行，并且会话服务器720存储应用程序的工作状态以及应用程序正在处理的任何数据。在另一实施例中，在用户断开之后，会话服务器720可以选择地停止特定应用程序的执行。例如，在一个实施例中，会话服务器720继续执行应用程序一个固定时间段，并且如果用户不能在那个时间段内连接，那么会话服务器720停止该应用程序。在另一实施例中，会话服务器720不使用任何用户输入停止不能继续执行的特定应用程序会话。在每个上面所述的实施例中，如果第一客户端节点702的用户从服务器726断开并且然后连接到服务器726同时操作第一客户端节点702、第二客户端节点716、或第三客户端计算机，则会话服务器720可以连接由用户操作的客户端计算机到一个或多个先前发起的与用户有关的未终止的一个或多个应用程序会话，并且重新发起任何停止的应用程序的执行。

[0108] 在一个实施例中，会话服务器720检测到断开。用户可以有意和手工命令服务器从用户正在与之通信的客户端节点702或716断开应用程序会话。例如，在一个实施例中，应用程序会话提供用户可以选择的用于断开(与上面的终止有所区别)的菜单选项。会话服务器720还可以检测无意断开。例如，在一个实施例中，会话服务器720识别何时传送到客户端节点702或716的预定数量的数据分组还没有由客户端节点702或716确认。在另一实施例中，客户端节点702或716定期传送信号给服务器726来确认连接仍旧保持原样。如果会话服务器720检测到来自客户端节点702或716的预定数量的预期确认信号还没有到达，那么会话服务器720确定客户端节点702或716已经断开。如果会话服务器720检测到用户已经从应用程序会话有意或无意地断开，那么与断开的应用程序会话有关的会话服务器720中的项目被修改来反映该断开。

[0109] 在接收到认证信息之后，会话服务器720查阅所存储的应用程序数据库722来识别与用户有关但连接到不同客户端节点比如举例来说第一客户端节点702的任何有效应用程序会话。在一个实施例中，如果会话服务器720识别任何这样的有效应用程序会话，那么会话服务器720自动地将一个(或多个)应用程序会话与第一客户端节点702断开并且连接该一个(或多个)应用程序会话到当前客户端计算机716。在一些实施例中，所接收的认证信息将限制客户端节点702重新连接到的应用程序会话。在一个实施例中，用户可以触发会话服务器的自动查阅以及随后与单个用户接口元件的选择的连接。

[0110] 在识别与客户端节点702有关的应用程序会话之后，会话服务器720连接客户端节点702到相关的应用程序会话。会话服务器720确定所述多个应用程序会话中的每一个是有效还是断开的。在一个实施例中，所述多个应用程序会话中的至少一个是有效的。在一个实施例中，所述多个应用程序会话中的至少一个是断开的。在一个实施例中，会话服务器720

自动接收应用程序输出。在另一实施例中，应用程序输出的接收由客户端节点702触发单个用户接口元件的选择。会话服务器720基于包含在所接收的信息714中的访问控制决定识别与客户端节点702重新连接的断开的应用程序会话。在一个实施例中，一旦识别任何断开的应用程序会话，则会话服务器720提示用户表示是否希望连接。如果不希望连接，则会话服务器720提示用户表示断开的应用程序会话是否应当保持断开，或者应用程序会话是否应当终止。

[0111] 在一个实施例中，连接包括修改所存储的应用程序数据库722中的项目以表示用户被连接到应用程序会话并且表示用户从那个客户端节点702连接到服务器。一旦连接，服务器726重新开始传送应用程序输出数据到客户端节点702或716。在一个实施例中，与客户端节点有关的所述多个应用程序会话在连接之前被连接到第一客户端节点702并且，在连接之后所述多个应用程序会话被重新连接到第一客户端节点702。在另一实施例中，与所述客户端节点有关的所述多个应用程序会话在连接之前被连接到第一客户端节点702并且，在连接之后所述多个应用程序会话被重新连接到第二客户端节点716。

[0112] 下面的示例性例子示出了上面讨论的方法和设备如何被用于提供基于政策的对客户端节点的文件内容的访问。这些例子用于示例而不是用来限制本发明。

[0113] 证据收集

[0114] 在一个实施例中，客户端节点102请求访问位于政策机106所位于的同一网络的服务器上的文字处理文档。政策机106接收请求并且确定它不拥有任何关于客户端节点102的信息。政策机106传送收集代理104到客户端节点102。在一些实施例中，收集代理104具有从客户端节点进行收集的预定义信息。在其它实施例中，收集代理104首先分析客户端节点来确定将要收集什么类型的信息。在又一个实施例中，收集代理104从政策机106取回关于将要收集关于客户端节点102的什么信息的指令。

[0115] 一旦在客户端节点102上执行，则收集代理104收集所请求的信息并且传送该信息112给政策机106。政策机106接收信息112并且开始确定信息112满足什么条件的处理。在一些实施例中，政策机106确定所接收的信息112不足够用于确定信息112是否满足一个或多个条件。在那些实施例中，政策机106传送另外的指令给收集代理104用于收集关于客户端节点102的更多信息。

[0116] 基于政策的访问控制

[0117] 当政策机106的第一部件202确定满足一个或多个条件时，它存储每个满足条件的标识符到数据组中。一旦完成，第一部件202传送该数据组以及所请求的应用程序给第二部件210。在这个实施例的一个例子中，所请求的应用程序可以是文字处理文档并且所满足的条件可以表示客户端设备是个人数字助理。在这个实施例的另一个例子中，所请求的应用程序可以是电子制表软件并且所满足的条件可以表示客户端设备是从不安全网络比如公共互联网公用电话亭连接的受信任的膝上型计算机。在这个实施例的第三个例子中，所请求的应用程序可以是添加到电子邮件消息的文件并且所满足的条件可以表示客户端设备在从安全网络连接的但缺少适当的应用程序软件来观看该文件的个人桌上型计算机上。

[0118] 第二部件210从第一部件202接收数据组并且应用一个或多个政策到所接收的数据。在这个实施例的一个例子中，第二部件210可以应用政策，该政策要求当客户端设备类型为个人数字助理时如果客户端节点在其上具有应用程序软件的条件不满足，则客户端节

点接收转换的文件内容。客户端节点将然后接收能够连接到转换服务器的可执行文件，转换服务器将以对于客户端设备类型可访问的格式呈现文件内容。应用这个政策使得客户端节点能够观看文件内容，而不管用于观看的不适当形式因素。

[0119] 在这个实施例的又一个例子中，第二部件210可以应用政策，当客户端设备类型为受信任的膝上型计算机时该政策禁止下载到客户端节点102，所述膝上型计算机包含适当的但来自不安全网络比如互联网公用电话亭的应用程序软件。在这个实施例中，政策可能要求政策机106传送可执行文件给客户端节点102，客户端节点102使得能够连接到应用程序服务器416以用于呈现文件内容。应用这个类型的政策并且取回文件仅给应用程序服务器416，使得客户端节点102能够观看文件内容而不危及来自不适当散布的私有文件内容。

[0120] 在这个实施例的又一个例子中，第二部件210可以应用政策，该政策要求个人桌上型计算机做出安全连接，但缺乏适当的应用程序软件，通过ICA会话将个人桌上型计算机连接到应用程序服务器416，并且要求应用程序服务器416执行适当的应用程序并且将该文件呈现给客户端节点102。应用该政策使得客户端节点102能够观看文件内容而不管在客户端节点102上是否缺少应用程序软件。

[0121] 本发明可以提供为包含在一项或多项产品上或在一项或多项产品中的一个或多个计算机可读程序。所述项产品可以是软盘、硬盘、光盘、数字多能光盘、高速存储器卡、PROM、RAM、ROM、或磁带。一般而言，计算机可读程序可以以任何编程语言来实现。可以使用的语言的一些例子包括C、C++、C#、或JAVA。软件程序可以被存储在一项或多项产品上或在一项或多项产品中作为目标代码。

[0122] 虽然已经参照特定优选实施例加以示出和描述了本发明，但是本领域的技术人员应当理解，可以在形式和细节上对其做出各种变化而不背离下面权利要求所限定的本发明的宗旨和范围。

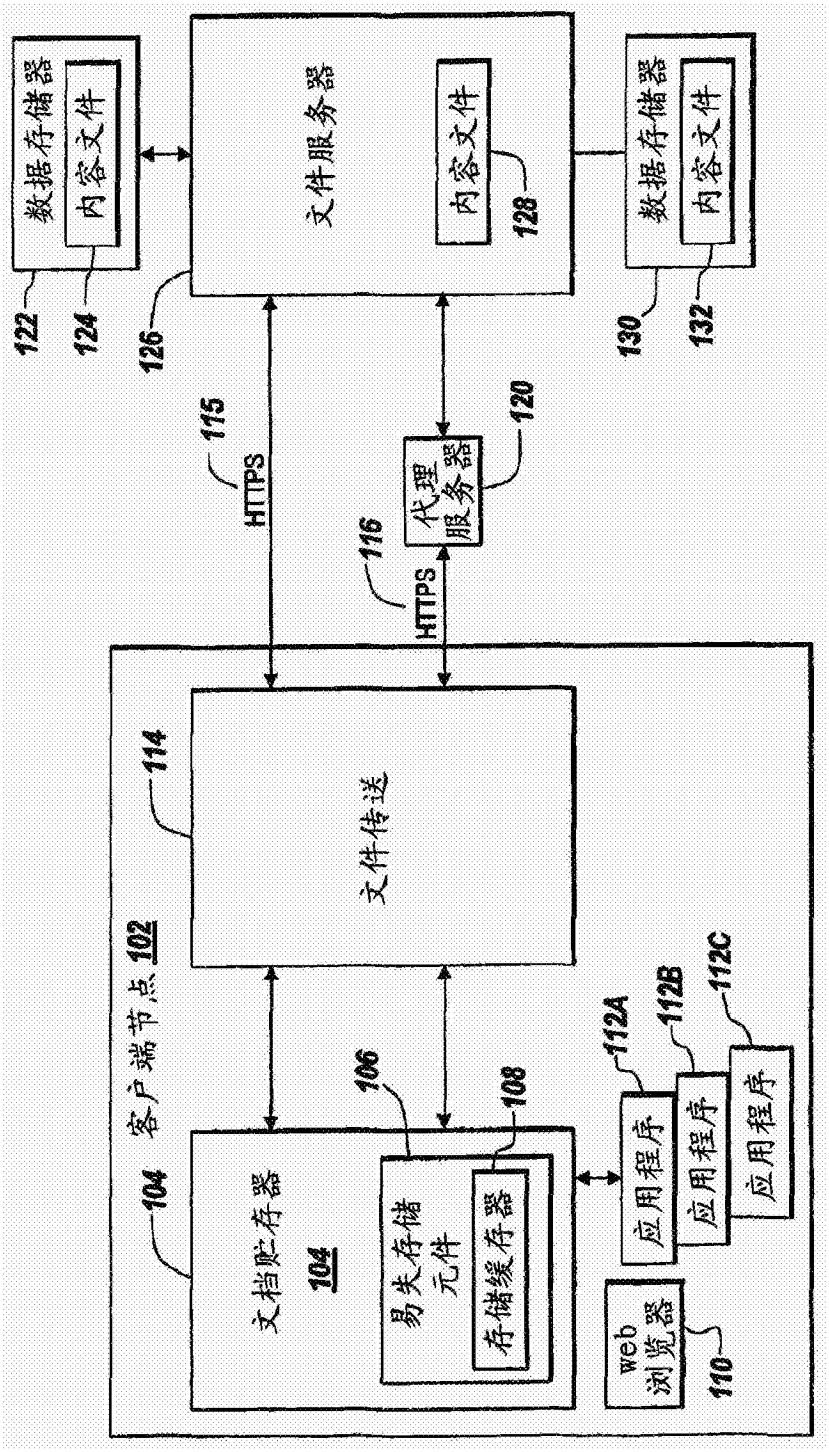

数据存储器
内容文件
122
124
文件服务器
126
内容文件
128
数据存储器
内容文件
130
132
115
HTTPS
116
HTTPS
代理服务器
120
客户端节点 102
114
文件传送
104
文档贮存器
104
106
易失存储元件
存储缓存器
108
112A
应用程序
112B
应用程序
112C
应用程序
web浏览器
110

图1A

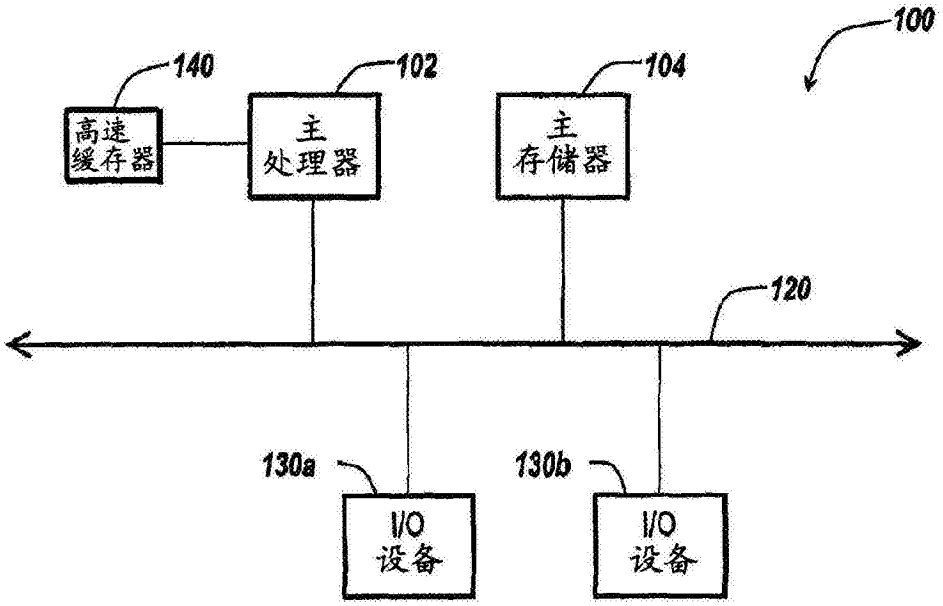

100
140
高速缓存器
102
主处理器
104
主存储器
120
130a
I/O设备
130b
I/O设备

图1B

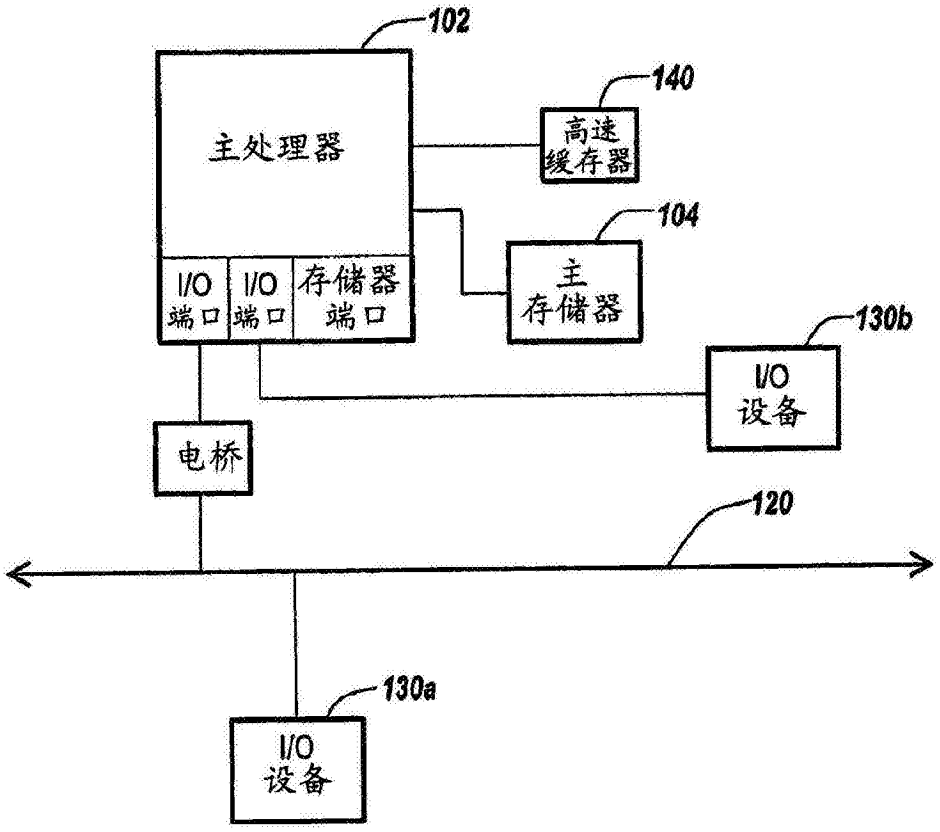

102
主处理器
I/O端口
I/O端口
存储器端口
140
高速缓存器
104
主存储器
130b
I/O设备
电桥
120
130a
I/O设备

图1C

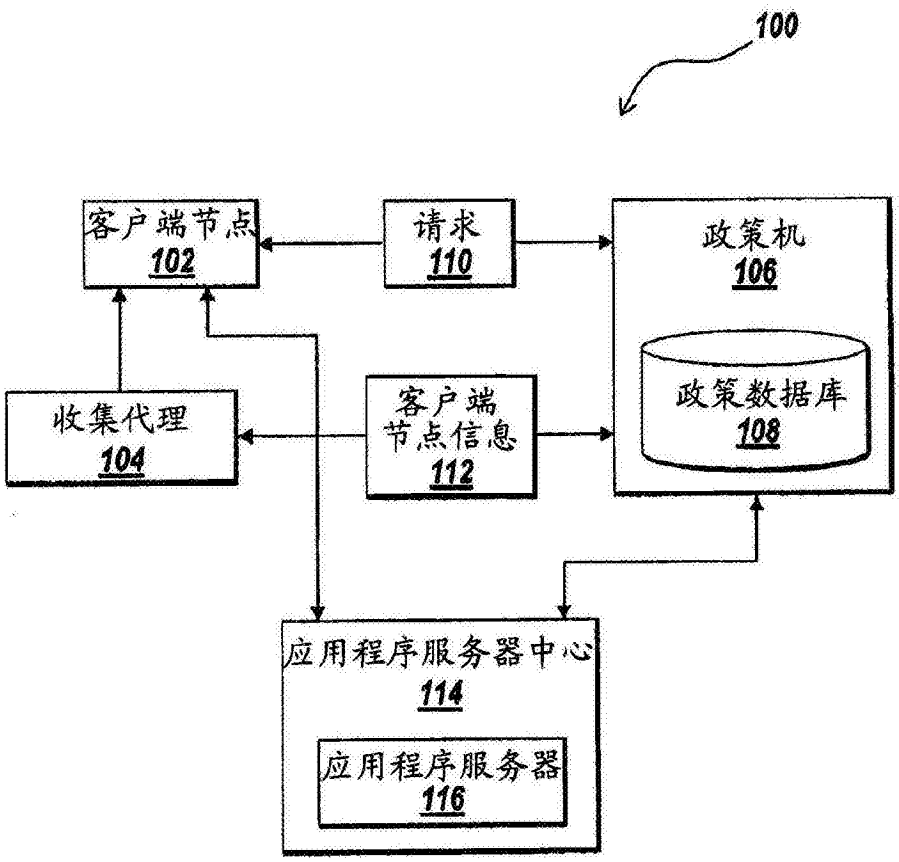

100
客户端节点
102
请求
110
政策机
106
政策数据库
108
收集代理
104
客户端
节点信息
112
应用程序服务器中心
114
应用程序服务器
116

图1D

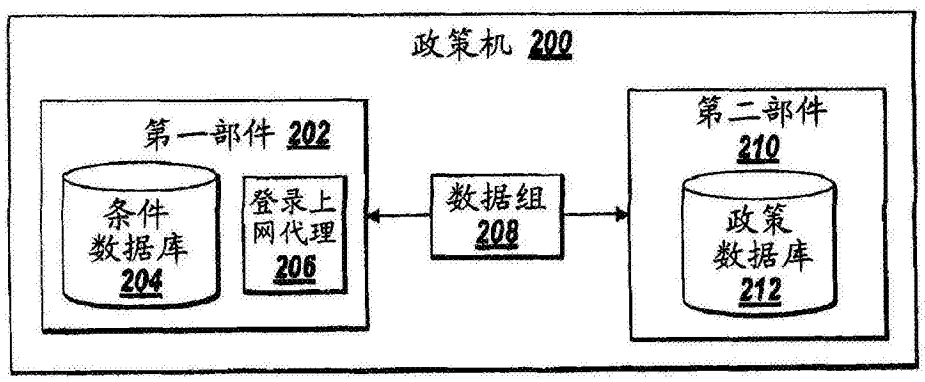

政策机 200
第一部件 202
条件
数据库
204
登录上
网代理
206
数据组
208
第二部件
210
政策
数据库
212

图2

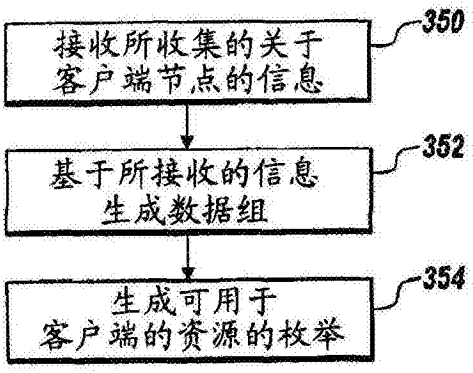

接收所收集的关于客户端节点的信息
350
基于所接收的信息生成数据组
352
生成可用于客户端的资源的枚举
354

图3

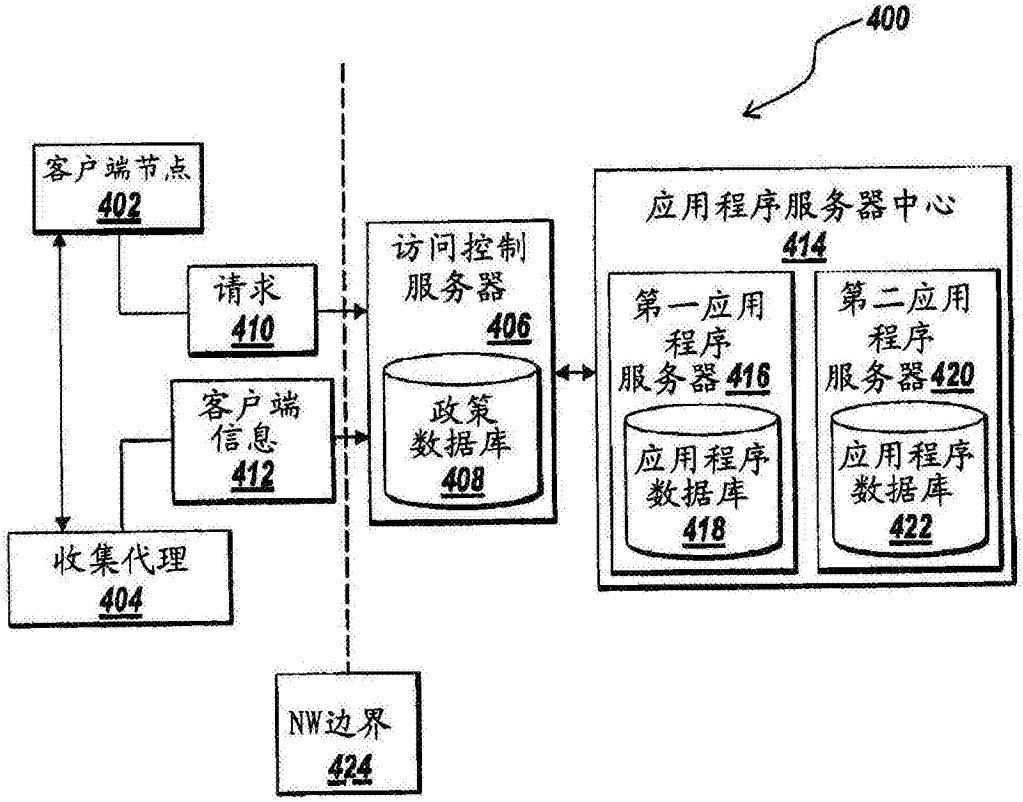

400
客户端节点
402
请求
410
客户端信息
412
收集代理
404
访问控制服务器
406
政策数据库
408
NW边界
424
应用程序服务器中心
414
第一应用程序服务器416
应用程序数据库
418
第二应用程序服务器420
应用程序数据库
422

图4

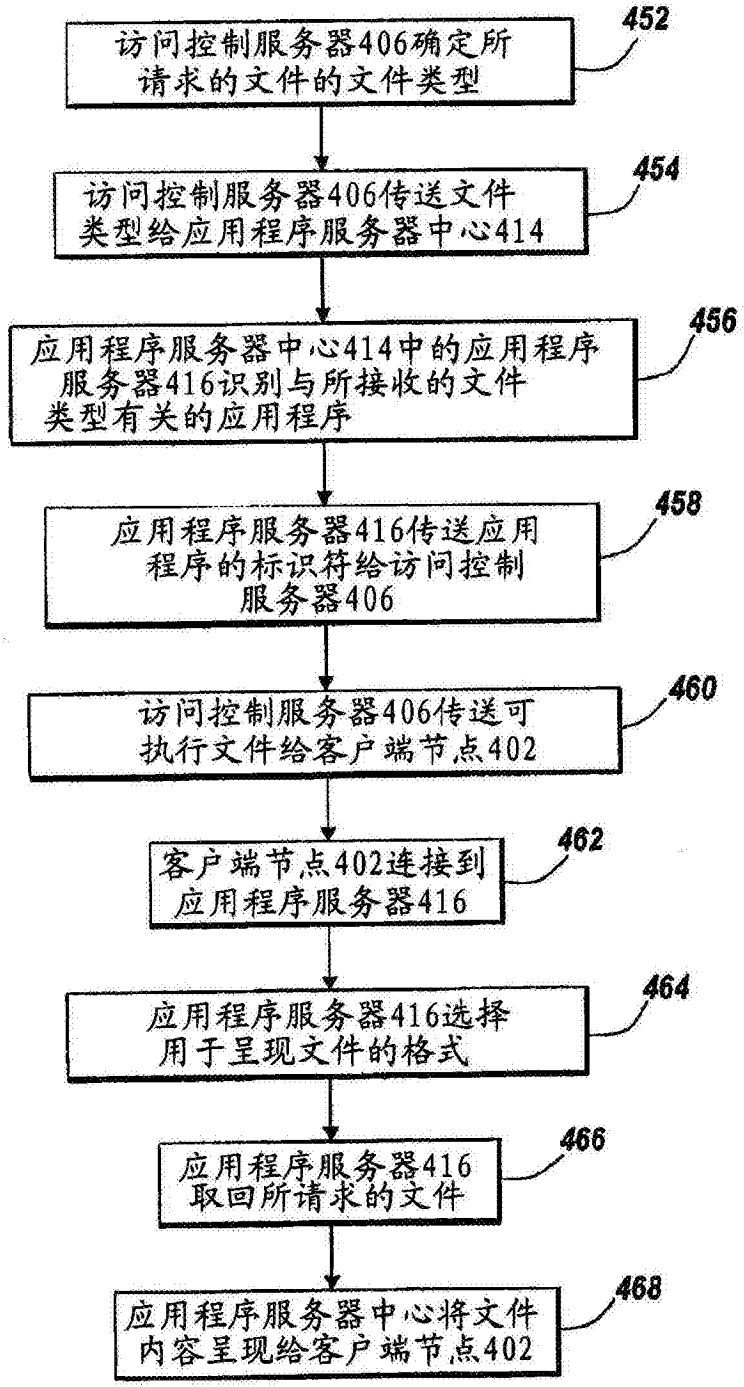

访问控制服务器406确定所请求的文件的文件类型
452
访问控制服务器406传送文件类型给应用程序服务器中心414
454
应用程序服务器中心414中的应用程序服务器416识别与所接收的文件类型有关的应用程序
456
应用程序服务器416传送应用程序的标识符给访问控制服务器406
458
访问控制服务器406传送可执行文件给客户端节点402
460
客户端节点402连接到应用程序服务器416
462
应用程序服务器416选择用于呈现文件的格式
464
应用程序服务器416取回所请求的文件
466
应用程序服务器中心将文件内容呈现给客户端节点402
468

图4B

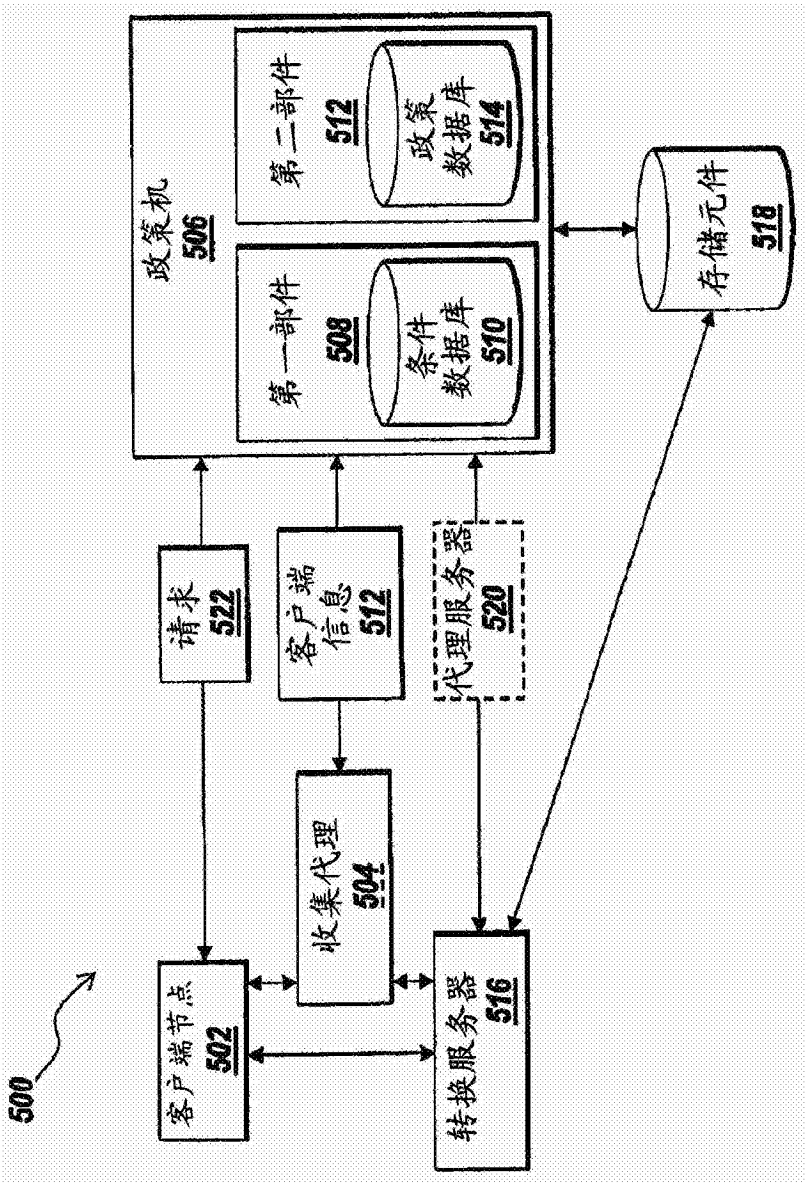

500
客户端节点
502
收集代理
504
转换服务器
516
请求
522
客户端信息
512
代理服务器
520
政策机
506
第一部件
508
条件数据库
510
第二部件
512
政策数据库
514
存储元件
518

图5

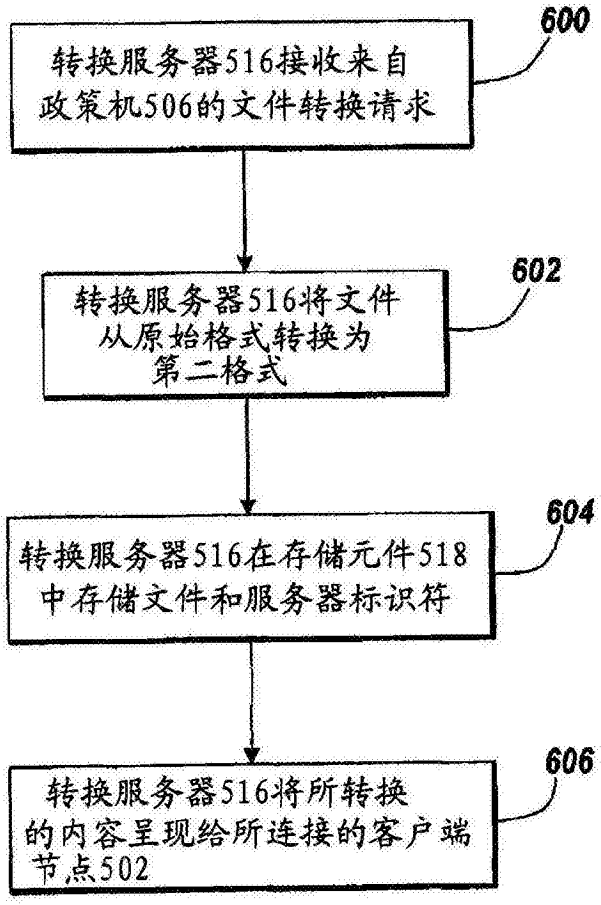

600
转换服务器516接收来自政策机506的文件转换请求
602
转换服务器516将文件从原始格式转换为第二格式
604
转换服务器516在存储元件518中存储文件和服务器标识符
606
转换服务器516将所转换的内容呈现给所连接的客户端节点502

图6

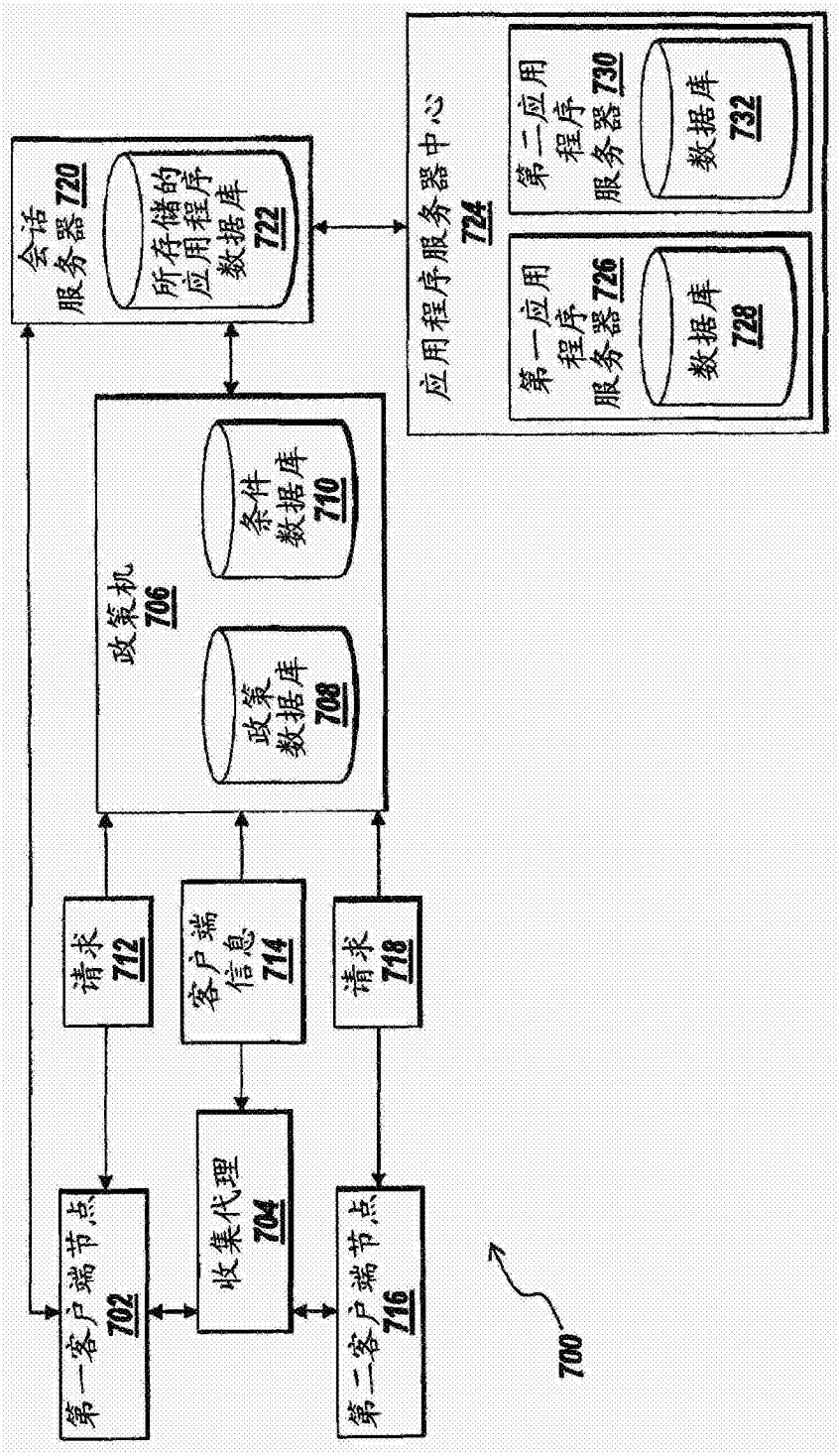

会话
服务器 720
所存储的
应用程序
数据库
722
应用程序服务器中心
724
第一应用
程序
服务器 726
数据库
728
第二应用
程序
服务器 730
数据库
732
政策机
706
条件
数据库
710
政策
数据库
708
请求
712
客户端
信息
714
请求
718
第一客户端节点
702
收集代理
704
第二客户端节点
716
700

图7

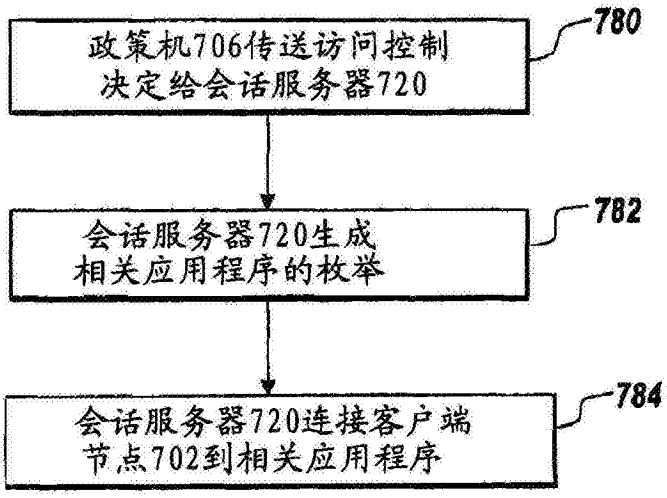

政策机706传送访问控制
决定给会话服务器720
780
会话服务器720生成
相关应用程序的枚举
782
会话服务器720连接客户端
节点702到相关应用程序
784

图7B