

技术概述

Feb. 23, 2016

XenApp 和 XenDesktop 是虚拟化解决方案。利用这些方案，IT 可以在提供随时随地访问任何设备的同时，控制虚拟机、应用程序、许可和安全性。

XenApp 和 XenDesktop 允许：

- 最终用户独立于设备的操作系统和界面运行应用程序和桌面。
- 管理员管理网络并提供或限制对选定设备或全部设备的访问。
- 管理员从单个数据中心管理整个网络。

XenApp 和 XenDesktop 共享统一的体系结构 FlexCast Management Architecture (FMA)。FMA 的关键功能是可以透过单个站点和集成置备运行多个版本的 XenApp 或 XenDesktop。

FMA 的关键功能

典型的 XenApp 或 XenDesktop 环境包括几项关键技术组件。这些组件在用户连接到应用程序和桌面时相互作用，并记录有关站点活动的的数据。

Citrix Receiver: 一款安装在用户设备上的软件客户端，通过 TCP 端口 80 或 443 提供与虚拟机的连接，并使用 StoreFront Service API 与 StoreFront 通信。

Citrix StoreFront: 用于对用户进行身份验证、管理应用程序和桌面并托管应用程序存储的接口。StoreFront 使用 XML 与 Delivery Controller 通信。

Delivery Controller: XenApp 或 XenDesktop 站点的中央管理组件，由用于管理资源、应用程序和桌面的服务组成，负责优化和平衡用户连接的负载。

Virtual Delivery Agent (VDA): 安装在运行 Windows 服务器或 Windows 桌面操作系统的计算机上的代理，允许这些计算机及其所托管的资源供用户使用。在运行 Windows 服务器操作系统的计算机上安装的 VDA 允许此计算机托管多个用户的多个连接，并通过以下其中一个端口连接到用户：

- 如果启用 TLS: TCP 端口 80 或端口 443
- 如果启用了通用网关协议 (CGP) (用于启用会话可靠性): TCP 端口 2598
- 如果禁用 CGP 或用户使用旧版客户端进行连接: TCP 端口 1494

Broker Service: 一种 Delivery Controller 服务，用于跟踪登录的用户和登录位置、用户拥有的会话资源以及用户是否需要重新连接到现有应用程序。Broker Service 执行 PowerShell 并通过 TCP 端口 80 与 Broker Agent 通信。它不可以使用 TCP 端口 443。

Broker agent: 托管多个插件并收集实时数据的代理。 Broker Agent 位于 VDA 上并通过 TCP 端口 80 连接到 Controller。 它不可以使用 TCP 端口 443。

Monitor Service: 一种 Delivery Controller 组件，用于收集历史数据并在默认情况下将其存放在站点数据库中。 监视服务通过 TCP 端口 80 或 443 通信。

ICA 文件/堆栈: 捆绑的用户信息，在连接到 VDA 时需要此信息。

站点数据库: Microsoft SQL Server 数据库，用于存储 Delivery Controller 的数据，如站点策略、计算机目录和交付组。

NetScaler Gateway: 数据访问解决方案，使用其他凭据在 LAN 防火墙内外提供安全访问。

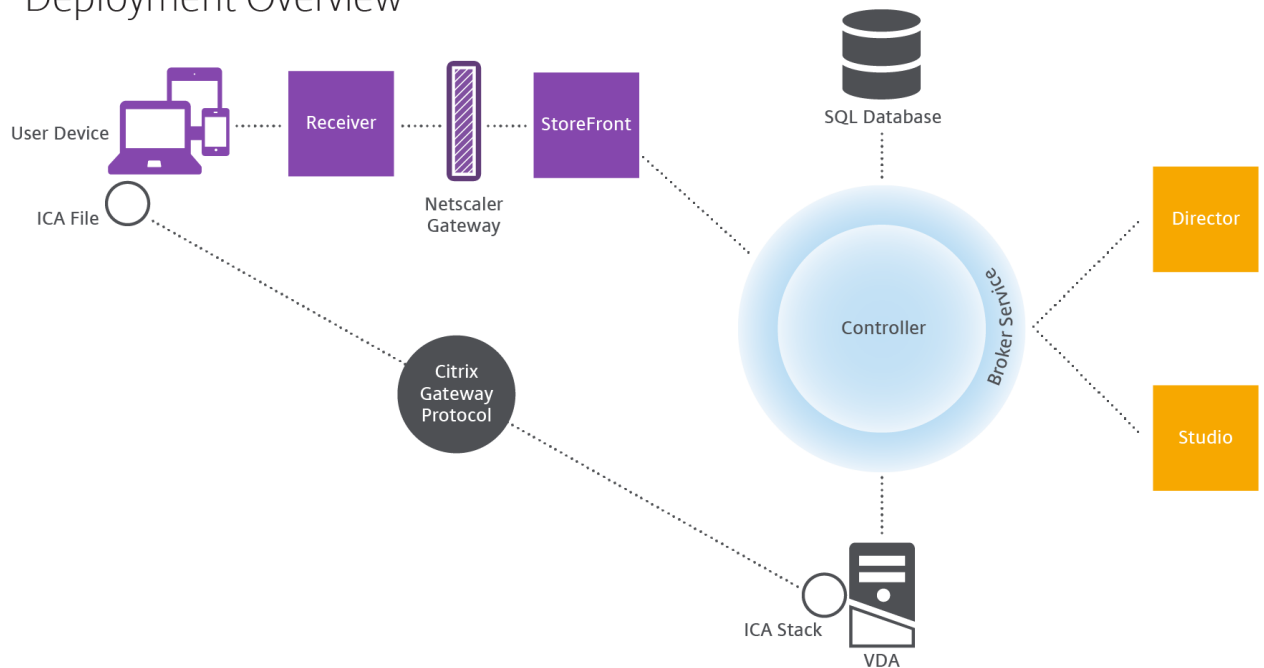
Citrix Director: 基于 Web 的工具，允许管理员和技术支持人员访问 Broker Agent 的实时数据、站点数据库中的历史数据和 NetScaler 中的 HDX 数据，以进行故障排除和提供支持。 Director 通过 TCP 端口 80 或 443 与 Controller 通信。

Citrix Studio: 管理控制台，允许管理员配置和管理站点，授予对 Broker Agent 中的实时数据的访问权限。 Studio 通过 TCP 端口 80 与 Controller 通信。

典型部署的工作原理

XenApp 和 XenDesktop 站点由具有专用角色的计算机组成，用于实现可扩展性、高可用性和故障转移，并提供设计安全的解决方案。 XenApp 或 XenDesktop 站点包括安装 VDA 的服务器和桌面计算机，以及用于管理访问权限的 Delivery Controller。

Deployment Overview



VDA 使用户能够连接到桌面和应用程序。它安装在数据中心内的服务器或桌面计算机上以实现大多数交付方法，但是也可以安装在物理 PC 上以实现 Remote PC Access。

Controller 由独立的 Windows 服务组成，用于管理资源、应用程序和桌面，并优化和平衡用户连接。每个站点具有一个或多个 Controller，并且，由于会话依赖延迟、带宽和网络可靠性，在理想状态下，所有 Controller 应该位于相同 LAN 上。

用户绝对不能直接访问 Controller。VDA 充当用户和 Controller 之间的媒介。当用户使用 StoreFront 登录到站点时，其凭据被传递到 Broker Service。Broker Service 根据为用户设置的策略获取其配置文件和可用资源。

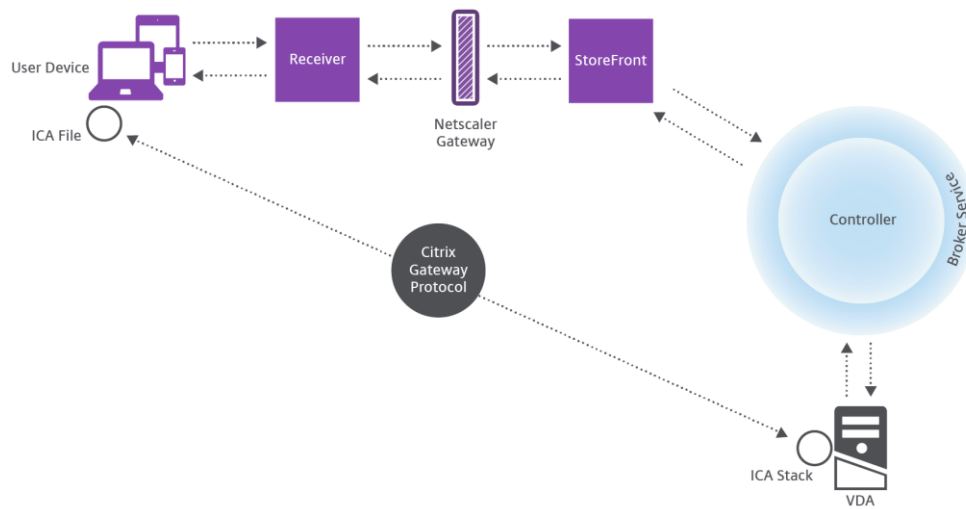
用户连接的处理方式

要启动 XenApp 或 XenDesktop 会话，用户通过 Citrix Receiver（安装在用户设备上）或 Citrix Receiver for Web (RFW) 进行连接。

在 Citrix Receiver 内部，用户选择所需的物理或虚拟桌面或虚拟应用程序。

用户的凭据按照此路径进行传递以访问 Controller，后者通过与 Broker Service 通信确定所需的资源。建议管理员在 StoreFront 上放置一个 SSL 证书以加密来自 Receiver 的凭据。

User connections



Broker Service 决定允许用户访问的桌面和应用程序。

验证凭据后，有关可用应用程序或桌面的信息通过 **StoreFront-Citrix Receiver** 路径发送给用户。用户选择此列表中的应用程序或桌面时，该信息按照相反路径返回到 **Controller**，**Controller** 决定托管特定应用程序或桌面的 **VDA**。

Controller 将用户的凭据通过消息发送给 **VDA**，并将关于用户和连接的所有数据发送给 **VDA**。**VDA** 接受连接，并将该信息按原路径返回给 **Citrix Receiver**。**Citrix Receiver** 将会话中已生成的所有信息绑定在一起，从而在用户设备上（如果 **Citrix Receiver** 安装在本地）或 **Citrix RFW** 上（如果通过 **Web** 访问）创建 **Independent Computing Architecture (ICA)** 文件。只要站点经过正确设置，凭据在整个流程均保留加密状态。

ICA 文件被复制到用户设备上，并在设备与 **VDA** 上运行的 **ICA** 堆栈之间建立直接连接。此连接绕过管理基础结构：**Citrix Receiver**、**StoreFront** 和 **Controller**。

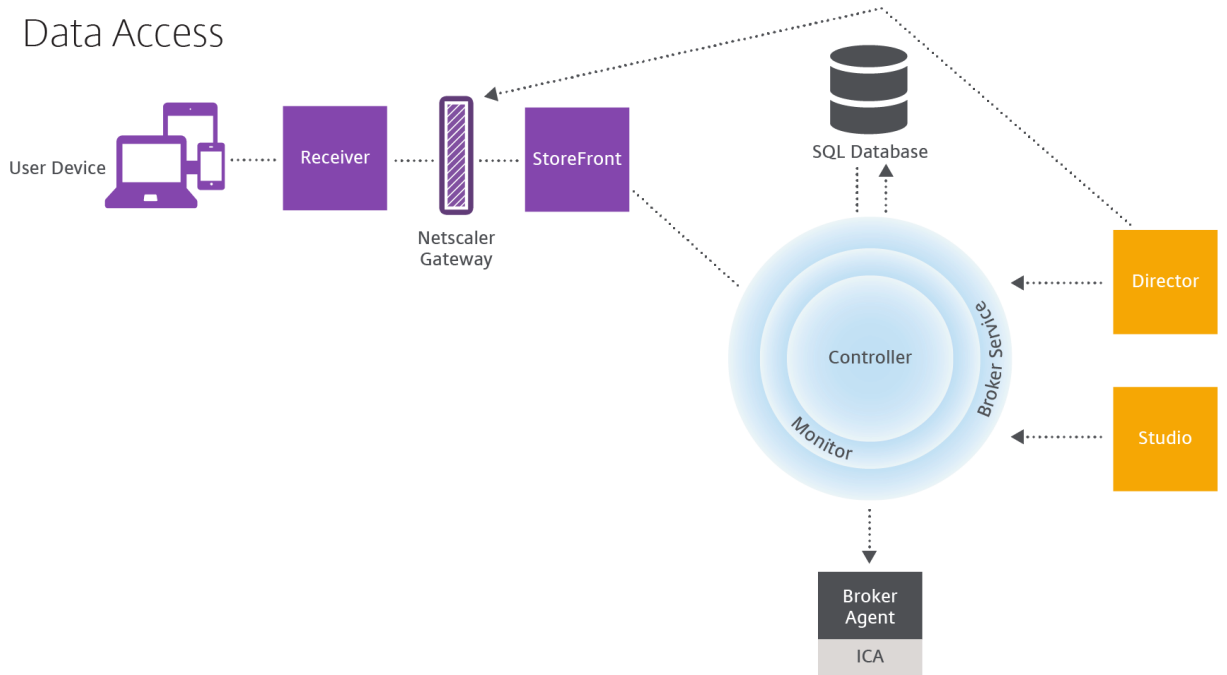
Citrix Receiver 和 **VDA** 之间的连接使用 **Citrix Gateway Protocol (CGP)**。如果连接丢失，通过会话可靠性功能，用户可以重新连接到 **VDA**，而无需通过管理基础结构重新启动。可以在 **Studio** 中启用或禁用会话可靠性。

客户端连接到 **VDA** 后，**VDA** 会通知 **Controller** 用户已登录，**Controller** 将此信息发送到站点数据库，并开始在监视数据库中记录数据。

数据访问的工作方式

IT 可以通过 **Studio** 或 **Director** 访问每个 **XenApp** 或 **XenDesktop** 会话生成的数据。**Studio** 允许管理员访问 **Broker Agent** 中的实时数据，以便更好地管理站点。**Director** 可以访问此实时数据、存储在监视数据库中的历史数据以及 **NetScaler Gateway** 中的 **HDX** 数据，用于提供技术支持和故障排除。

Data Access



在 **Controller** 内部，**Broker Service** 报告虚拟机上的每个会话的会话数据，以提供实时数据。 监视服务还跟踪实时数据并将其作为历史数据存储于监视数据库中。

Studio 只能与 **Broker Service** 通信，因此也只能访问实时数据。 **Director** 可以与 **Broker Service** 通信（通过 **Broker Agent** 中的插件）以访问站点数据库。

Director 还可以访问 **NetScaler Gateway** 以获取 **HDX** 数据信息。