

# Luccitech智能流量调度白皮书

鸿鹄科技（深圳）有限公司|www.LucciTech.com

LucciTech

让应用更快、更安全、更智能

目录

一、前言 ..... 3
1、本方案致力于解决零信任架构下应用系统的信任问题 ..... 3
2、方案特点 ..... 3
3、智能流量调度解决的问题如下 ..... 3
一、Luccitech智能流量调度的安全性 ..... 4
1、数据传输安全 ..... 4
2、统一登录窗口安全 ..... 5
3、系统安全 ..... 5
二、Luccitech智能流量调度的扩展性 ..... 5
1、性能 ..... 5
2、第三方认证系统的扩展 ..... 6
3、信息系统的扩展 ..... 6
4、安全架构的扩展 ..... 6
三、统一身份认证 ..... 6
1.单因素论证 ..... 6
2.双因素论证(MFA) ..... 9
四、用户访问控制 ..... 11
1.不同用户组的访问界限 ..... 11
2.同一信息系统的匿名访问界限 ..... 11
3.同一信息系统的访问界限 ..... 12
4.用户组分流 ..... 12
5.指定用户访问 ..... 12
五、单点登录 ..... 12
1.内置单点登录 ..... 12
2.第三方单点登录集成 ..... 13
六、信息系统的加速 ..... 13
七、安全合规 ..... 13
1.功能列表 ..... 14
2.系统列表 ..... 15
3.功能和系统的映射 ..... 15
八、产品核心能力 ..... 27
九、核心功能特性 ..... 28
十、安全与扩展性 ..... 29
十一、性能指标 ..... 30
十二、高可用与负载均衡 ..... 31
十三、公司介绍 ..... 31

## 一、前言

### 1、本方案致力于解决零信任架构下应用系统的信任问题

- 应用的统一身份认证
- 应用的统一身份权限
- 应用数据传输的完整性和私密性

### 2、方案特点

- 统一应用安全防护
- 统一用户登录体验
- 统一应用身份权限
- 无缝本地向云迁移
- 适配现有应用环境
- 高性能的横向扩展
- 应用性能数据导出

安全认证的核心是身份验证和授权,解决的是用户是否合法以及用户访问信息系统的权限这两个问题。

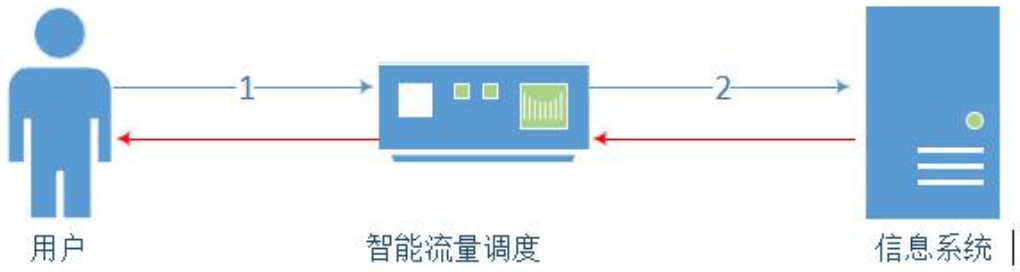
随着云计算的发展，越来越多用户将应用迁移到云平台上，同时保留部分应用(数据)到本地私有云或数据中心，在这种混合环境下，安全认证对应用安全的重要性得到提升：解决信息系统采用传统网络边界进行安全管理带来的问题，比如 VPN，用户通过 VPN 访问内网，整个内网都暴露给用户。

### 3、智能流量调度解决的问题如下

- 智能流量调度自身的安全性
- 智能流量调度的扩展性
- 信息系统的统一身份认证
- 信息系统的用户访问控制

- 信息系统的单点登录
- 信息系统的加速
- 安全合规

所有的信息系统通过 Luccitech智能流量调度发布，所有从用户到信息系统的数据均经过Luccitech智能流量调度。




## 一、Luccitech智能流量调度的安全性

Luccitech智能流量调度作为所有信息系统的统一入口，以反向代理的方式将所有信息系统隐藏在后面，避免了信息系统直接被攻击的可能性。

Luccitech智能流量调度成为整个系统架构的第一道防线，也是被攻击的第一个目标，因此智能流量调度自身的安全性显得尤为重要。

**Luccitech智能流量调度的自身安全性包括三个方面：**

### 1、数据传输安全

- 所有客户端和 Luccitech智能流量调度之间的数据传输，全部采用 SSL/TLS 加密，加密协议默认采用 TLS 1.2，安全证书采用 2048 bit；并提供 SSL/TLS 加密的弹性机制：支持 TLS 1.3， 4096bit 证书，自定义加密套件，HSTS 标签，客户端数字证书透传。
- Luccitech智能流量调度和第三方认证系统的数据传输支持加密，比如和 AD 认证支持 StartTLS
- 或 LDAPS 加密协议，和 SAML 身份提供方如AD FS 认证支持

m-TLS 双向数字证书验证。

- Luccitech智能流量调度和信息系统之间，考虑到加密对信息系统的性能影响，默认采用明文传输；但是支持从 Luccitech智能流量调度和信息系统之间的数据传输加密。
- Luccitech智能流量调度和信息系统之间的安全认证支持 Kerberos。

**2、统一登录窗口安全**

- 支持人机识别，避免机器人攻击。
- 支持登录失败次数/账户锁定以及超时自动登出。
- 支持设定公网/私网登录方式。
- 登录窗口的 URL 自动生成一次性 Token 字符串避免被盗刷。
- 登录窗口的用户名/密码均采用私有算法加密。

**3、系统安全**

- Luccitech智能流量调度采用 DPDK 开发，并非基于标准 Linux 内核，在提升性能的同时，其精简的架构也最大程度保证系统本身的安全性。

## 二、Luccitech智能流量调度的扩展性

Luccitech智能流量调度作为所有信息系统的统一入口，其扩展性决定了整个架构的扩展性，包括如下四个方面：

**1、性能**

- Luccitech智能流量调度采用 DPDK 技术，其处理数据包的性能是标准Linux内核的 10 倍，单机最大的七层吞吐支持 40Gbps。
- 支持 SSL 硬件加速，2048bit的单机每秒 SSL 新建连接支持12万，4096bit的单机每秒 SSL新建连接支持2万4千。
- Luccitech智能流量调度支持集群 N+1 部署，集群数量和性能成正比，集群最大支持 16 台设备, 最大支持 600Gbps 吞吐，2048bit 的每秒 SSL 新建连接支持 180 万，4096bit 的单机每秒SSL 新建连接支持 36

万。

- Luccitech智能流量调度支持 HA 冗余部署，避免单点故障。

**2、第三方认证系统的扩展**

- 支持第三方认证系统的横向扩展，比如，支持将多个 AD 作为认证源。

**3、信息系统的扩展**

- 提供专业的服务器负载功能，便于信息系统自身的横向扩展，信息系统的扩展对于用户和网络架构是透明的。

**4、安全架构的扩展**

- 提供高性能的 SSL 卸载功能，将 HTTPS 加密数据包自动转换为 HTTP 明文，其他安全设备如 WAF，IPS 等可以部署在Luccitech智能流量调度后面，从而整个安全架构中，只需要做一次HTTPS 解密即可，避免 WAF 等安全设备再做 HTTPS 解密导致的整个网络性能降低。




**三、统一身份认证**

Luccitech智能流量调度提供多种统一身份认证机制，满足不同业务场景对于应用安全的管理需求。身份认证通常指验证用户是否合法，但在安全等级高的环境，同时需要验证信息系统是否合法。

**1.单因素论证**

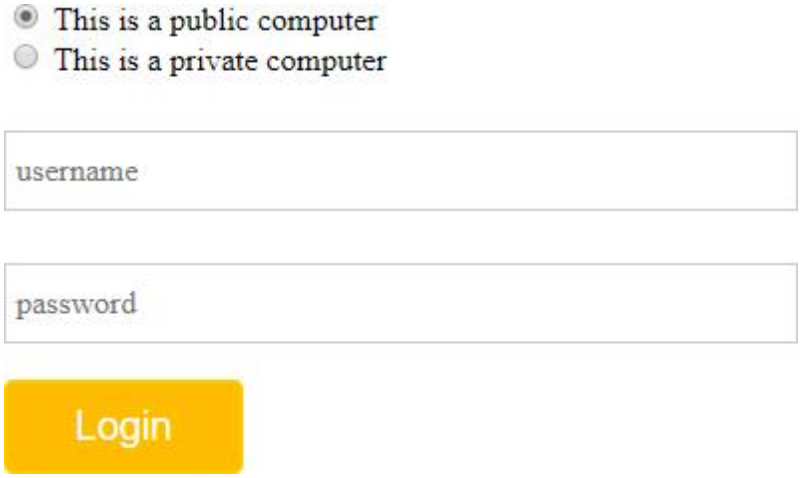
这种业务场景是内网多个信息系统需要对外发布，但是身份认证只采用单一的账户系统作为认证源。

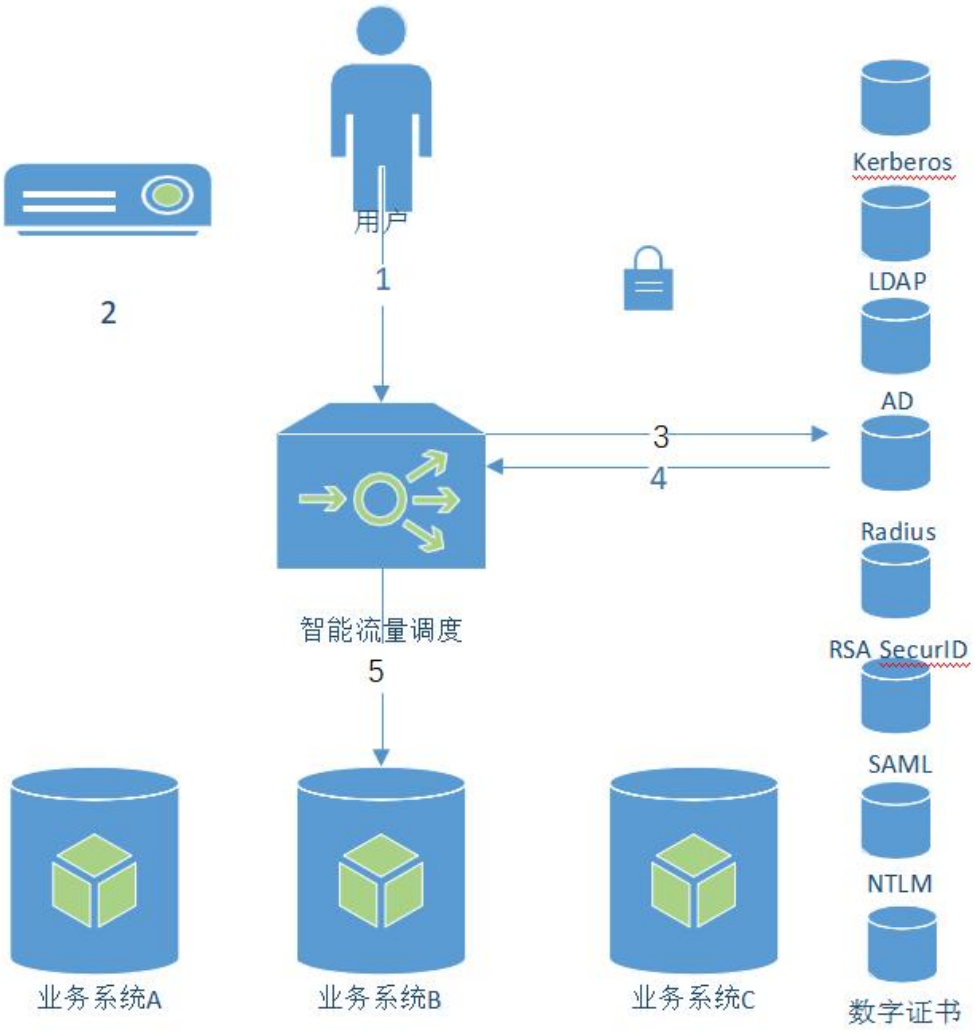
Luccitech智能流量调度支持多种第三方认证协议做单因素认证，包括 LDAP, Radius，NTLM,SAML, RAS SecurID，数字证书服务，Kerberos。

单因素论证通常有两种实现方式，第一是通过登录窗口，第二是通过客户端的数字证书。

**登录窗口：**

这种方式比较常见，当用户访问通过 Luccitech智能流量调度发布的信息系统时，当第一次登录或超时，会弹出一个登录窗口，如下图：



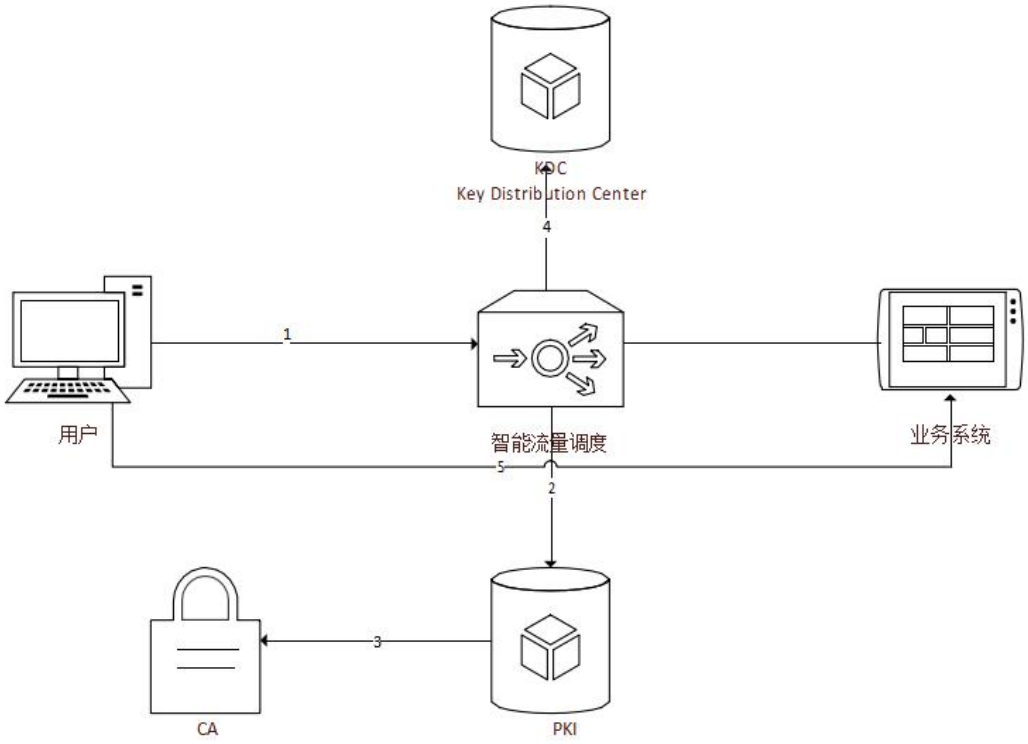



**工作流程如下：**

- 用户开始访问业务系统
- 对该用户弹出登录窗口，用户输入用户名/密码
- 把用户名/密码发给第三方论证系统进行验证
- 验证成功
- 该用户允许访问业务系统 A，同时，可以访问业务系统B 和 C，不需要重新进行认证

**客户端数字证书认证：**

也称为 m-TLS，即需要同时验证服务端和客户端的数字证书，通常用于对于安全性要求非常高的业务场景，比如公安系统。



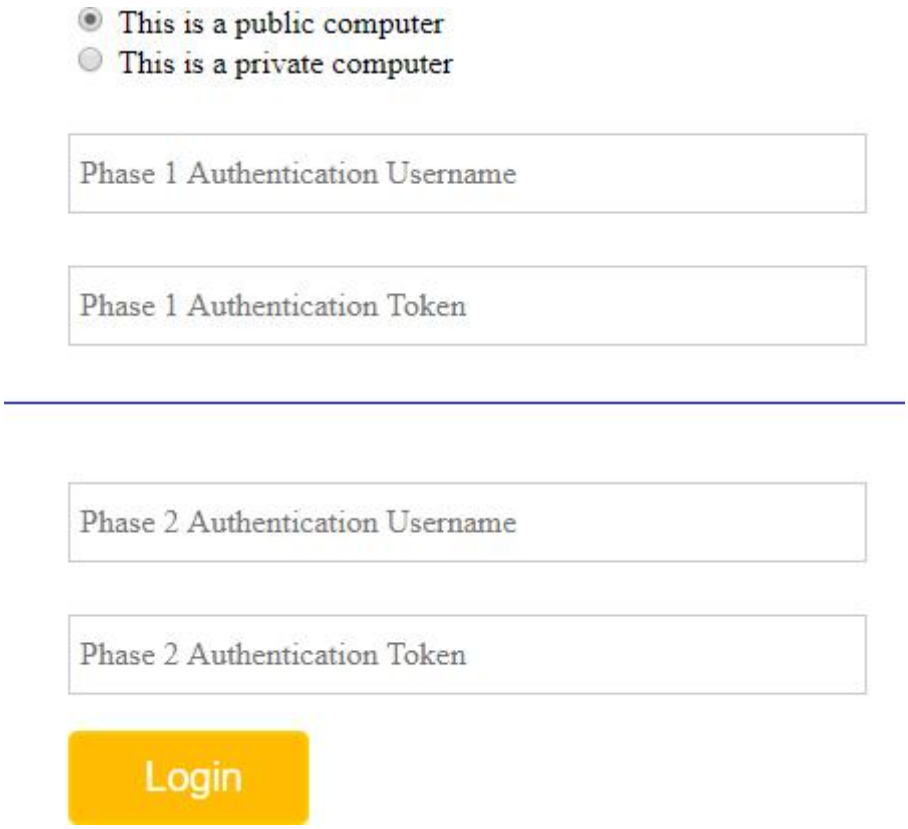

**工作流程如下：**

- 在客户端手工安装数字证书(或 USB Key 数字证书),用户通过 HTTPS 访问业务系统,Luccitech智能流量调度请求客户端提交数字证书
- Luccitech智能流量调度通过 OCSP 协议和 PKI 通信,验证该客户端的数字证书是否合法
- PKI 向 CA 权威机构发起请求,对客户端数字证书的合法性进行校验
- Luccitech智能流量调度从客户端数字证书中提取 SAN(Subject Alternative Name)并和 LDAP 中用户的 UPN(User Principal Name)进行匹配.匹配成功后,Luccitech智能流量调度会从Kerberos 获取该用户的 service ticket(服务凭证)和访问的业务系统的 service ticket(服务凭证)
- 用户被授权访问业务系统

**2.双因素论证(MFA)**

这种业务场景是内网多个信息系统需要对外发布，但是身份认证采用两套账户系统作为认证源，最大程度保证应用的安全性。

双因素论证通常有两种实现方式，第一是在单因素认证的基础上，加入 OTP 一次性密码或验证码，通过短信或邮件等方式发给用户。第二种是登录窗口有对内和对外的两套账户密码， 如下图：




**支持的双因素认证协议如下：**

- Radius + LDAP
- RAS SecurID + LDAP

**3.跨域身份认证**

跨域的身份验证是指应用系统部署在不同的网络，比如有的信息系统部署在公有云平台， 有的则部署在本地数据中心或私有云。

Luccitech智能流量调度支持SAML 协议，SAML 有两个角色，服务提供方（SP，即Service Provider）和身份提供方（IdP，即 Identity Provider），其中身

份提供方承担了跨域的单点登录，身份认证和授权的功能，目前有不少厂家，比如微软的 AD FS 就是SAML 的身份提供方，将 AD 账户系统和 IdP 集成在一起，构成一个完整的跨域账户系统，统一身份认证和授权以及单点登录的 SAML 解决方案。

Luccitech智能流量调度是 SAML 服务提供方（SP），对于信息系统而言，只需要通过 Luccitech智能流量调度发布，就可以和现有的 SAML 身份提供商(IdP)集成，从而解决如下问题：

- 跨域（比如有的信息系统部署在校园网，有的信息系统部署在云平台）的身份验证和授权问题。
- 账户系统的集中和本地管理
- 跨域的统一身份验证和授权的安全性问题

**4.信息系统认证**

信息系统的合法性认证是安全信任的一部分，信息系统默认用户是不可信任的，同样用户也默认信息系统是不可信任的。

Luccitech智能流量调度支持通过 Kerberos 协议和信息系统进行认证。

**四、用户访问控制**

用户访问控制是对用户进行信息系统的授权访问，本质是用户组和信息系统的访问映射关系。Luccitech智能流量调度支持如下用户访问控制：

**1.不同用户组的访问界限**

用户登录后,基于其所属用户组的信息系统访问控制.比如用户组 1 只能访问信息系统 A 和 B,而用户组 2 只能访问信息系统C 和 D

**2.同一信息系统的匿名访问界限**

同一个信息系统,可以指定根据信息系统的不同部分(URL),有的需要身份验证,有的面向公众不需要身份验证.比如网站面向公众开放不需要身份验证,但是

网站的资料下载页面需要内部员工的权限才可以访问。

**3.同一信息系统的访问界限**

同一个信息系统,可以指定根据信息系统的不同部分(URL)指定不同的用户组权限.比如用户访问的 URL 是 oa.test.com/marketing,则需要市场部用户组权限,如果访问的 URL 是 oa.test.com/hr 则需要人事部用户组的权限才可以访问。

**4.用户组分流**

同一个信息系统有多台服务器,可以指定根据不同的用户组访问信息系统不同的服务器。

**5.指定用户访问**

对于安全性非常高的信息系统,支持在指定电脑(在该电脑上安装数字证书)+指定 IP 才能访问。

**五、单点登录**

Luccitech智能流量调度本身提供单点登录功能，也支持和第三方单点登录系统进行集成。

**1.内置单点登录**

Luccitech智能流量调度内置单点登录提供如下功能：

- 支持多个单点登录域，同一个单点登录域下的信息系统只需要登录一次
- 自定义单点登出
- 自定义单点登录的 Session 时间
- 自定义单点登录窗口页面
- 自定义单点登录窗口登录失败最大次数/锁定时间
- 支持密码代填方式实现信息系统的自动登录

**2.第三方单点登录集成**

Luccitech智能流量调度提供 API 实现和第三方单点登录进行集成。

## 六、信息系统的加速

Luccitech智能流量调度支持 WEB 信息系统的加速，通过 HTTP/2 和 HTTP/1.1 的自动转换，实现信息系统和用户数据的二进制传输压缩和连接复用，使得：

- 信息系统的访问速度提升 30-50
- 消耗的带宽减少 1/3
- 大幅减少服务器的并发连接




## 七、安全合规

根据等保 2.0 <网络安全等级保护基本要求> GB/T 22239 一 2019 的等保三级要求 8.1.2.2

8.1.2.2 通信传输

本项要求包括：

a) 应采用校验技术或密码技术保证通信过程中数据的完整性；

b) 应采用密码技术保证通信过程中数据的保密性。

Luccitech智能流量调度的 SSL 卸载可以确保通信过程中的加密要求。上一个例子是介绍智能流量调度提供信息系统统一身份验证和授权的基本工作流程。第二个例子是从整个应用环境来看智能流量调度的工作流程。身份验证和授权是复杂的，涉及到多个系统和跨域环境，下面介绍基本概念。

首先，我们需要厘清三个基本的问题

- 信息系统的统一身份验证和授权，哪些功能是必不可少？我们需要定义一个功能列表
- 信息系统的统一身份验证和授权，哪些系统是必不可少的？我们需要定义一个系统列表
- 功能列表和系统列表的映射关系

**1.功能列表**

- 信息系统的入口管理
- 用户身份验证
- 信息系统权限控制
- 单点登录/登出
- 信息系统身份验证
- 日志审计



**2.系统列表**

- 账户系统（必须），所有账户均保持在该系统中
- 单点登录系统（必须），用于提供所有信息系统的统一身份验证和单点登录
- 用户权限控制系统（必须），用于管理信息系统的访问权限和用户的映射和授权
- 信息系统身份验证系统（可选），对于安全要求高的网络环境，除了要验证用户合法，还必须验证信息系统合法，Kerberos 是常用的标准协议
- 信息系统（必须）
- 智能流量调度（必须）

**3.功能和系统的映射**

这个映射根据实际网络环境而不同，有的网络环境没有单点登录系统，有的网络环境已经有除了智能流量调度之外的所有系统。

我们智能流量调度提供除了信息系统和账户系统之外的所有系统功能，即我们智能流量调度可以作为单点登录系统，用户控制系统，信息系统身份验证系统和智能流量调度。根据实际环境定义这个映射是确定我们智能流量调度在整个网络环境中需要做什么，和不做什么。

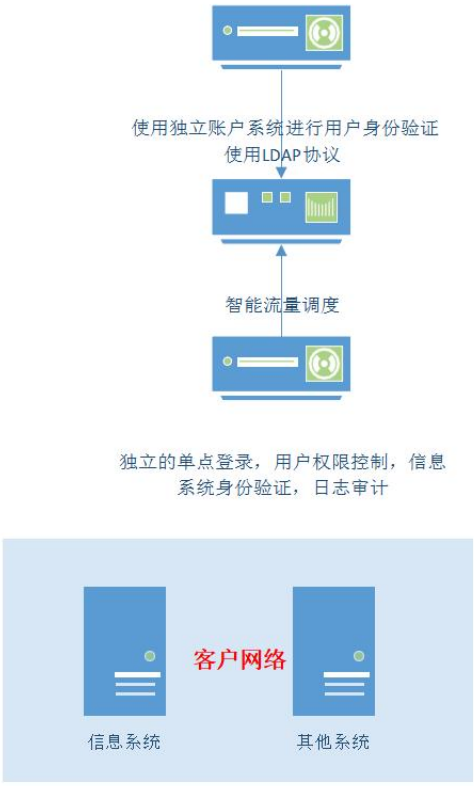
**我们产品的思路：**

针对这种复杂的应用环境，最复杂的地方在于不同系统之间的集成，而信息系统的开发有时候不会严格遵循通信标准，使得问题更加复杂化。举个例子，一个高校用户把学生账户信息同步到新星学习通，就算高校想把账户系统保留到本地，让新星学习通通过高校本地的账户系统进行身份验证，可能都无法实现，比如新星学习通的登录机制基于 MYSQL 的某个表查询，只能把高校的学生账户导入到 MYSQL 的那个表中。再比如其他在线学习云平台，弄个基于 ORACLE 的某个表查询，又需要把高校的学生账户导入到 ORACLE 的某个表中。这样会

导致账户系统完全失控。问题的根源在于没有遵循统一的标准比如 LDAP，RADIUS 等。

所以，我们产品采用两种办法尽量规避类似情况的出现：

- 我们产品的核心功能均采用独立结构，完全独立于客户环境中的现有网络和应用，你可以想象成我们产品和现有网络的关系，就是 OSI 模型中第七层应用和第四层网络的关系。这样就最大程度避免了现有网络的交互。




举例来说，单点登录功能在我们产品上是独立的，我们针对用户这一端实现功能，这样无论客户网络是否实现了单点登录，用户权限控制等，对我们都没有影响，比如客户网络已经有单点登录，这并不妨碍我们对用户做单点登录。

- 严格遵循标准，如下是我们使用和支持的标准：

| 功能 | 标准 | 说明 |
| --- | --- | --- |

| | | |
|---|---|---|
| 身份验证入口 | 浏览器 BASIC 验证<br>窗口标准 FORM 窗口<br>X.509 数字证书 | BASIC 窗口明文传输，不安全，不推荐使用。<br>X.509 数字证书用于安全性高的场景，比如云平台需要调用高校账户系统，那么我们可以使用数字证书来验证云平台的身份，不但安全， 而可以有效减少攻击，，没有安装数字证书无法和高校账户系统建立连接 |
| 账户系统 | LDAP<br>RADI<br>US<br>SAML<br>RSA SecurID<br>NTLM | 常用的是 LDAP，比如 AD 活动目录。<br>对于跨域的身份验证，采用<br>SAML |
| 身份授权 | LDAP<br>SAML | 跨域的身份授权，采用<br>SAML |
| 信息系统身份验证 | Kerberos | |
| 和现有单点登录或信息系统<br>的自动登录集成 | HTTP/1.1 POST | |

了解了以上这些背景，下面我们看第二个例子，我们假设用户已经有单点登录系统，那么按照功能和系统的映射关系，我们产品系统提供如下：

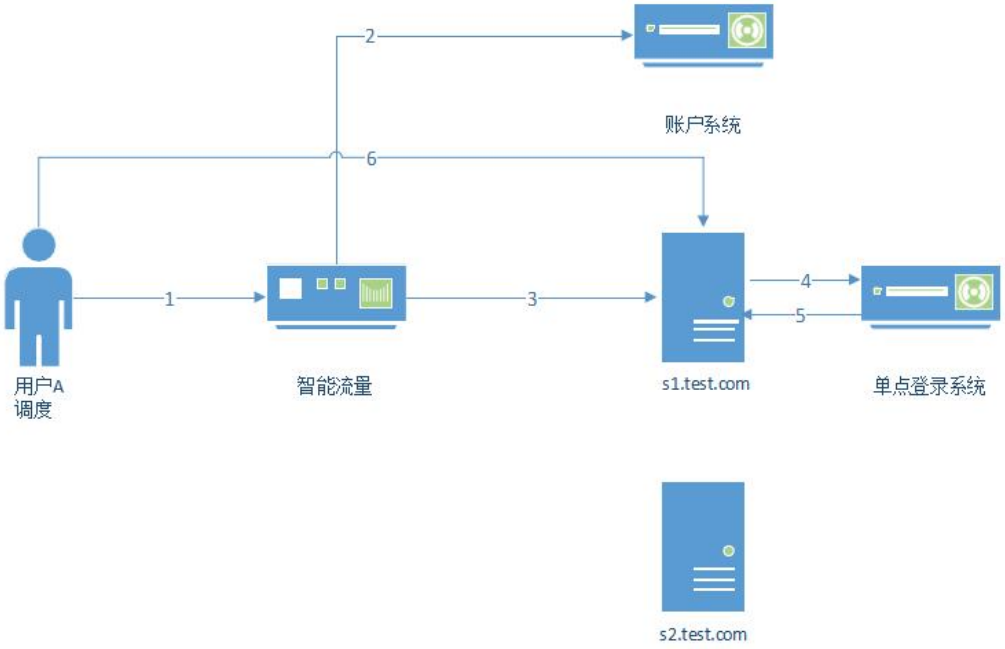
- 信息系统的入口管理
- 用户身份验证
- 集成现有的单点登录系统

- 信息系统权限控制
- 日志审计

为讨论方便，我们做如下假设：

| 用户 | 所属用户组 | 业务系统 | 说明 |
| --- | --- | --- | --- |
| 用户 A | 学生组 | 允许访问<br>s1.test.com<br>s2.test.com<br><br>禁止访问<br>t1.test.com<br>t2.test.com | 当用户 A 第一次访问s1.test.com，需要登录窗口进行身份验证，验证通过后，访问 s2.test.com 不需要再次身份验证。反之亦然。<br>当用户登出 s1.test.com，也同时自动登出 s2.test.com，反之<br>亦然。 |
| 用户 B | 教师组 | 允许访问<br>t1.test.com<br>t2.test.com | 当用户 B 第一次访问t1.test.com，需要登录窗口进行身份验证，验证通过后，访问 t2.test.com 不需要再次身份验证，反之亦然。<br>当用户登出 t1.test.com，也同时自动登出 t2.test.com，反之<br>亦然。 |

流程图如下：




**步骤如下：**

1.用户 A 访问 s1.test.com，该域名是由智能流量调度发布，指向服务器 s1.test.com.如果该用户 A 已经在访问 s1.test.com 或者 s2.test.com 登录论证通过，那么均可以直接访问。否则智能流量调度弹出登录窗口

2.用户 A 在登录窗口输入并提交，智能流量调度将用户 A 提交的用户名密码通过 LDAP 协议请求账户系统进行身份验证。验证成功后，匹配智能流量调度的用户组访问策略（即用户 A 允许访问 s1.test.com），上面两个步骤任何一个失败，登录窗口提示用户 A 验证失败。

3.智能流量调度使用事先定义好的 HTTP POST 策略以密码代填的方式将用户名密码提交

s1.test.com 实现自动登录

4.s1.test.com 将用户名和密码提交单点登录系统实现验证登录

5.单点登录系统接受到来自 s1.test.com 的登录请求，验证身份

6.用户 A 开始访问 s1.test.com

**这里需要注意：**

- 步骤 1，如果用户 A 访问 t1.test.com，那么就算用户 A 输入正确的用

户名密码，均不匹配智能流量调度的用户组访问策略（即用户 A 禁止访问 t1.test.com）

- 部署 4 和 5 的方式需要看单点登录的实际工作流程，有的是需要先登录单点登录。
- 步骤 6 独立于步骤 4 和 5，即无论步骤 4 和 5 返回的结果如何，均可以访问 s1.test,com
- 用户 B（教师组）的访问步骤类似

在这里，我们唯一需要和现有信息系统集成的就是步骤 3，用于实现自动登录，上面这个例子采用简单粗暴的密码代填方式，这样应对未采用标准论证协议的使用环境。我们支持标准协议kerberos 和SAML 和信息系统的单点登录集成。

关于标准协议，讲一点题外话。

网络开发和应用开发一个区别在于对标准协议的理解。网络开发面对的是开放的网络环境，一个数据包到达另外一端，中间经过若干节点的若干网络设备，如果不遵循 TCP/IP 协议，数据包都无法到达对端。而应用开放相对封闭，一个选课系统就是独立的系统，和其他系统交互有限或者没有，所以各显神通，遵循标准协议开发的动力不足，比如身份验证，采用 LDAP 等标准协议的不多。

但是随着云平台的发展，信息系统的边界从封闭走向开放，没有遵循标准协议的问题就放大了， 账户系统就是最开始浮现的问题，并不是说高校没有采用统一身份管理，而是缺乏对标准协议的使用和理解。

缺乏对标准协议的理解，会随着高校越来越多的使用云计算，各种各样的问题会层出不穷，这里面蕴藏着很多黄金市场。举个例子，对账户系统不同格式的合并，管理，同步的自动化，可能就可以做一个产品。

SAML 是应对异构环境和跨域身份验证授权的标准协议，我们第三个例子就是我们产品对SAML的支持。

第三个例子是我们产品对 SAML 的支持，解决的需求如下：

- 跨域（比如有的信息系统部署在校园网，有的信息系统部署在云平台）

的身份验证和授权问题。

- 账户系统的集中和本地管理
- 跨域的统一身份验证和授权的安全性问题这个

文档会涉及一些技术细节。

上面列出的需求，显然是一个普遍的问题，业界早已经有相关标准协议，在说明第三个例子之前，我们需要了解一些协议标准，这样就能理解为什么我们选择SAML。

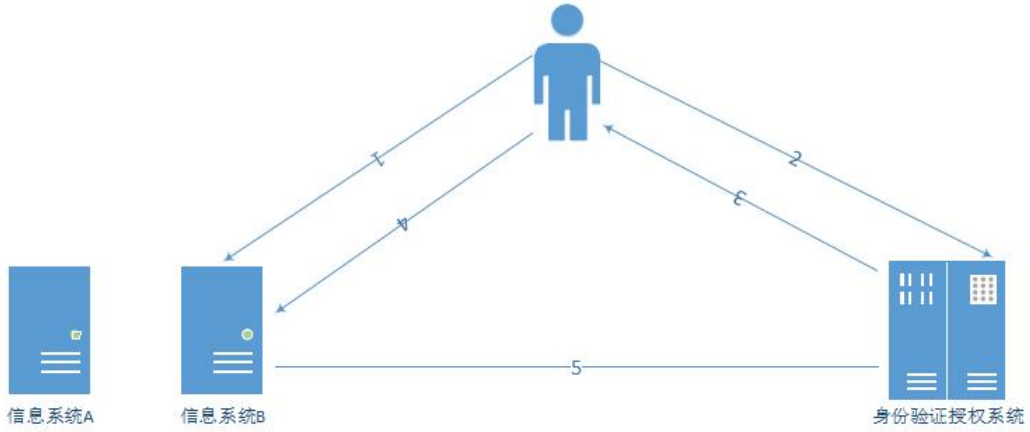
身份验证授权（含单点登录）最早是使用浏览器的 BASIC 认证，摘要认证和Cookie。

- BASIC 认证是用户向服务器发起请求，服务器返回 401 代码（Unauthorized），弹出一个窗口，用户输入密码后，在HTTP 报文插入字段Authorization: Basic Y291ZG90OnNlY3JldA==， Basic 后面就是Base64 加密的用户名:密码字符串。显然，这种方式完全不靠谱，用户名和密码字符串用 Base64 在网络传输，就是裸奔。网上那篇<详解如何构建零信任安全架构应用原型>就用 BASIC 认证，这个是不安全的。
- 摘要认证比 BASIC 认证安全一点，同样是服务器返回 401 代码（Unauthorized），通过服务器产生的随机数和客户端产生的随机数来进行用户名密码的验证，解决了 BASIC 认证通过网络明文传输密码的问题。
- 当然，还有依靠 Cookie 来进行身份认证的，通常使用 Set-cookie 报文。

这三种办法都不安全，而且只适合单个信息系统，没有办法扩展，遇到有多个信息系统要实现单点登录，身份验证授权这种需求，就无能为力，这也就是为什么现在基本上看不到这三个古董的原因。

解决这个问题的思路还是老办法，就是把身份验证授权从信息系统中抽离出

来，形成一个独立的控制中心系统，所有信息系统的身份验证授权都经过这个控制中心。这个思路在安全领域到处都是，我们产品作为信息系统的统一入口是这样，堡垒机作为运维管理系统的桥头堡也是这样。就是下面这个样子:




**工作流程如下：**

1.用户第一次访问信息系统

2.信息系统把请求丢给身份验证授权系统

3.身份验证授权系统为该用户生成临时令牌

4.用户接收到临时令牌并发给信息系统B 进行验证

上图中，信息系统和身份验证授权系统那条线就是我们要接下来讨论的，到底信息系统和身份验证授权系统是怎么交互的，由于涉及到众多的信息系统，不能乱来，肯定是需要一套标准的。

但有趣的是，标准的订立本身是一个乱来的过程，到 2020 年 3 月为止，已经有差不多 20 种身份验证/授权的标准，目前活下来的就是三个：CAS，SAML 2.0 和 OIDC（OpenID Connect）

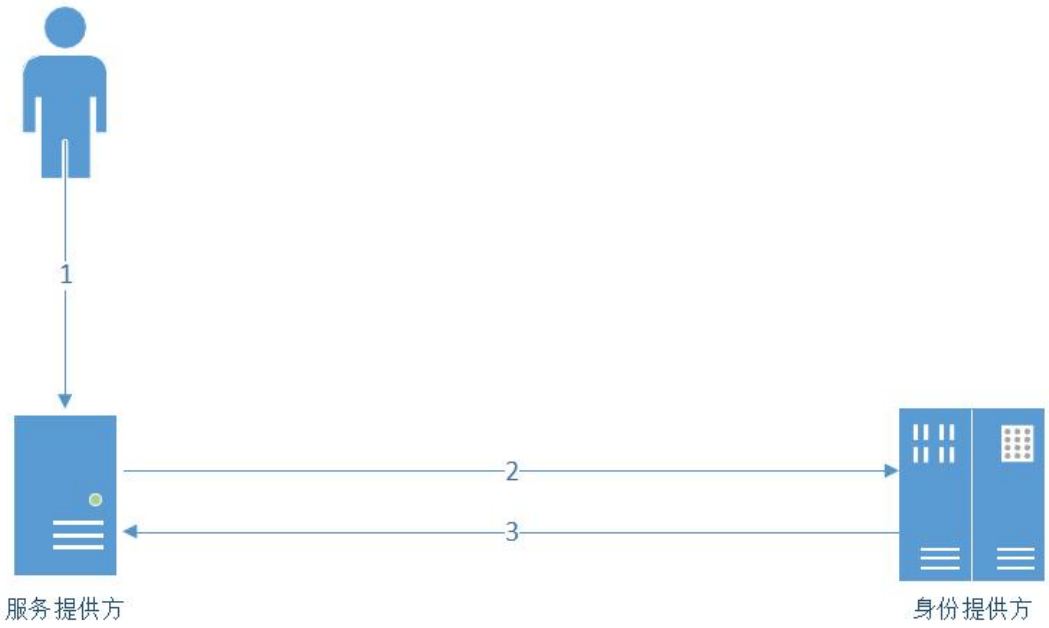
我们下面简单看看这三个协议，关于这三个协议的技术细节我们不展开，因为一百篇文档都无法涵盖这三个协议的技术细节。我们只列出这三个协议的适用场景：

- CAS 客户端和 CAS 服务器是没有强制安全要求的，安全性是三个协议中最弱的，而且CAS协议相对简单，适合于内部网络使用
- OIDC 基于 oAuth2，更适合面向公众的信息服务，比如 CSDN 网站，用户可以使用 QQ、微博或微信等第三方账户直接登录，注意，账户信息是来自第三方。OIDC 是 2014 年设立的， 集成了一些新技术包括 REST 和 JSON，对移动端的支持最好，安全性高，但是还处于发展阶段。
- SAML 是 2002 年设立，安全性高，成熟稳定，非常适合 SaaS 和跨域/混合云的场景，所以SAML 更适合面向企业（或高校），企业或高校肯定是需要建立自己的账户系统，不可能通过微信或 QQ 账户系统来维护学生老师的账户。但是 SAML 协议非常复杂。

基于上述原因，我们最终选择 SAML。

下面对 SAML 做一个背景介绍。

SAML 里面有三个主体，即用户，服务提供方和身份提供方。




工作流程如下：

1.用户向服务提供方（比如信息系统）发起访问请求

2.服务提供方生成 SAML 请求发给身份提供方

3.身份提供方对用户身份和权限进行验证，通过后生成 SAML 响应给服务

提供方

4.服务提供方允许用户访问

这里 SAML 有两个角色，服务提供方（SP，即 Service Provider）和身份提供方（IdP，即 Identity Provider），其中身份提供方是最关键的，它承担了跨域的单点登录，身份认证和授权的功能，目前有不少非常有实力的厂家，比如微软的 AD FS 就是 SAML 的身份提供方，将 AD 账户系统和 IdP 集成在一起，构成一个完整的跨域账户系统，统一身份认证和授权以及单点登录的 SAML 解决方案。

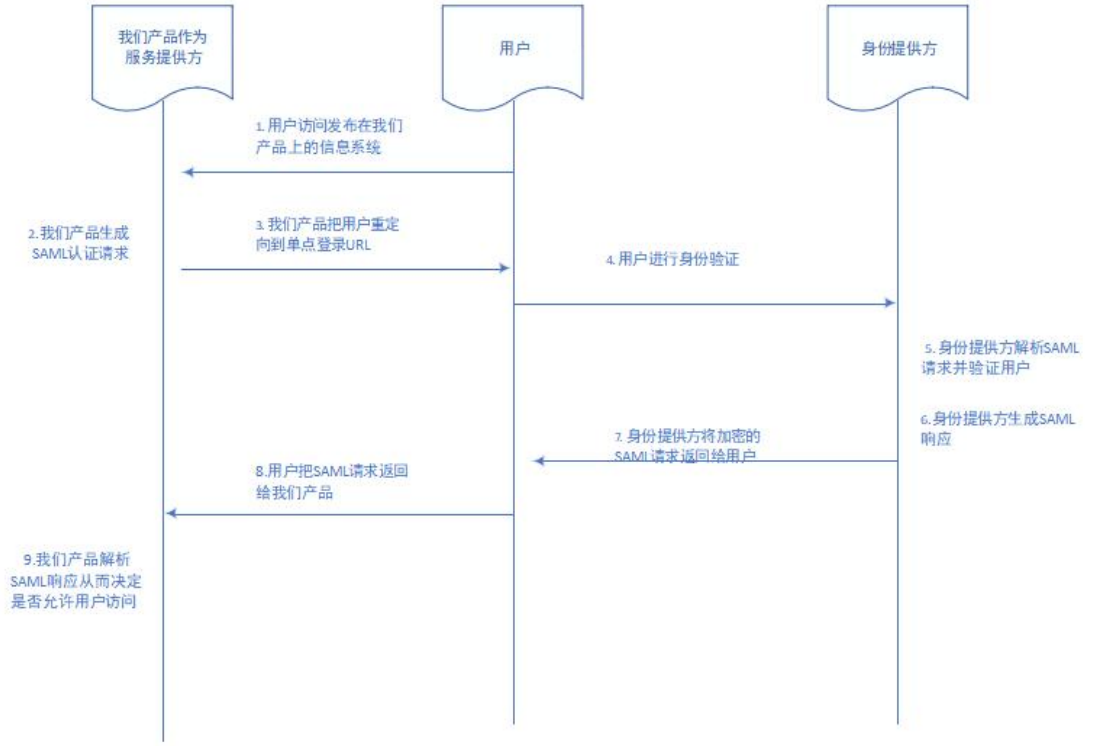
而我们产品是 SAML 服务提供方（SP），作为信息系统的发布方，和 SAML 的身份提供方（IdP）无缝集成，

我们的第三个例子通过支持 SAML，扩展到跨域/混合云环境下，单一本地账户应对众多信息系统的统一身份认证/授权和单点登录。

如下例子，我们以微软的 AD FS 作为SAML 的身份提供商，如果选择其他 SAML 身份提供商，工作机制是类似的。为讨论方便，我们做如下假设：

- 使用我们产品发布两个信息系统，s1.test.com 在校园网的数据中心，t1.test.com 在阿里云
- 两个信息系统的账户资料已经统一，并同步到校园网的 AD FS 服务器中
- 将两个信息系统的作为校园网 AD FS 的 Relying Party
- 阿里云部署 AD FS，并将阿里云的AD FS 作为校园网 AD FS 的 claims provider

具体工作流程图如下：




上图只有访问和授权的流程，单点登出（LOGOUT）的流程略。

第三个例子把 SAML 复杂的技术细节隐藏在我们产品，对于信息系统而言，只需要通过我们产品发布，就可以和现有的 SAML 身份提供商集成，从而解决本文档中最开始列出的需求。

关于身份认证授权和负载产品的一点题外话

SAML 发布 1.0 版本到现在有 18 年了，很多用户都没怎么听过，但为什么现在云平台都开始支持这个协议呢？可能还是两个原因，第一是复杂度，一个技术方案如果太复杂，接受程度就会降低，高校目前使用的 CAS 虽然有不少问题，但是在高校还是流行开了，其实从技术角度看， SAML 和 CAS 是两个完全不同量级的协议，SAML 强太多，但是 CAS 简单，弄起来方便。第二是使用场景，CAS 简单但是只适合内网使用，只要边界一扩展就不灵了，这也是 SAML 强大的地方，现在的跨域/混合云是 SAML 如鱼得水的。

SAML 协议是 2002 年开始的，居然适合现在云计算的场景，SAML 设计者的技术洞察力很了不起，这也说明了技术的本质并没有随着各种各样新技术的崛起发生大的变化。

我们产品最核心的就是负载，身份认证授权针对的是信息系统，而不是终端用户（象联软），真正的落脚点还是在信息系统的负载上面，现在负载的江湖变了，主要的变动有两点，第一是云计算，第二是 K8S 容器。负载的本质是连接网络和信息系统，网络变成了云平台，信息系统开发基于 K8S，等于负载连接的两头都发生了变化。对于传统的负载来说，有几点变化：

1. 性能变得不重要，云平台上可以随意扩充 VM 实例，或者在 K8S 上自动扩充 POD 实例，　　扩展性本身就是云平台的优势。

2. 快速部署变得重要，AWS 云平台自带的负载均衡占了 20　的市场份额，直接把 F5 这些厂　家打懵了，负载厂家都没有想到 AWS 那个简陋的负载能那么受市场欢迎，AWS 云平台刚推　出负载均衡，连会话保持都没有，负载调度算法也就三个，等大家回过味来，才发现快速部　署在云平台上的重要性。AWS 上建立一个负载均衡，点击一下就起来了。之所以快速部署很　重要，是业务系统的开发模式发生变化，DevOps 模式打破了开发和运维的界限，容器技术　将DevOps 的优势发挥的淋漓尽致。

3. DevOps 带来的另外一个影响是使用必须简化，想象一下在 F5 里面弄一个 iRules，没有半年　培训根本就用不起来，技术使用如果太复杂，对于 DevOps 来说，宁可牺牲功能，甚至连会　话保持这样重要的功能都可以牺牲，用来换取简化和效率。

基本上所有的负载厂家都错过了云平台的开始发展阶段，不过上面列出的问题，处理起来并不困难，现在主流的负载厂家在应对上面的 2#和 3#都做的不错，包括云平台版本，云平台上的模板，在云平台上的可扩展等等，无论技术怎么变化，应用系统的快速稳定安全的访问还是不会变的，这方面也是负载厂家安身立命的领域。

而且随着混合云的兴起，云平台上自带的负载均衡是无法应对的，需要同时管理云平台和私有云或本地数据中心的负载，所以负载厂家得到一个很好的市场机会。

我们产品之所以开发身份认证授权，其实主要针对的就是混合云的身份验证授权场景，信息系统的身份验证授权是应用安全的第一步，负载由于所处的网络位置，是最适合做这件事的，我们在垂直行业的云平台象 Oracle，SAP 都看到这一点，两者均提供云平台的身份验证授权。但是只是在云平台上做，如果是混合云就不好弄了，我们产品的身份认证授权就是解决这个问题。这也是我们支持 SAML 最根本的原因。

负载的本质是协议的支持，比云计算对负载更有影响的其实是协议，对于当前的负载来说，有三个协议是至关重要的。

1.HTTP 协议，因为主流的应用都是 WEB 应用，HTTP/0.9 到现在有进 30 年了，1997 年才推出 HTTP/1.1，一直用到现在。而到 2015 年才有 HTTP/2，负载的三大核心（健康检查，调度算法，会话保持）绝大部分均围绕 HTTP 协议开发。象太一星辰还在网站上写支持 SPDY 这个 HTTP/2 的前身协议，就可以看出他们的开发基本停止了。而真正会导致负载市场洗牌的是 HTTP/3，从 TCP 直接转到 UDP 上面，等于负载的三大核心都需要重新设计和开发。几年后这个影响就看的出来。

2.TLS 协议，现在最新的是 TLS 1.3，随着 HTTP/3 走 UDP，那么 TLS 协议也是需要重构。这个对于负载来说影响巨大。

3.VXLAN，这个协议在一般的网络看不出来，但是在大的数据中心，VXLAN 的协议支持是决定负载能否部署的前提

## 八、产品核心能力

Luccitech 智能流量调度平台（ADC）具备企业级跨云智能流量调度能力，集 SSL Termination、全局智能流量调度（GSLB）、DNS 服务于一体，通过专用 ASIC 芯片 SSL 加速器实现高性能 SSL/TLS 卸载，有效减轻后端服务器负担，提升整体业务处理效率。平台支持管理平面与数据平面分离的分布式架构，实现控制与转发解耦、故障域隔离及系统高可用与弹性扩展。同时，平台兼容裸金属、虚拟机、容器等多种部署形态，可根据不同环境灵活选择部署方式，满足企业多样化的基础设施需求。

## 九、核心功能特性

**1.多形态部署：**

支持全环境灵活部署支持，可无缝部署于裸金属物理服务器、VMware/KVM/Hyper-V 等主流虚拟化平台以及 Docker/Kubernetes 容器环境，针对不同部署环境提供对应的优化版本与部署工具，满足企业多样化的基础设施架构需求。弹性扩缩容：支持自动化弹性扩缩智能流量调度引擎，能够根据实时网络流量、服务器负载等多维度指标自动触发流量调度引擎的扩容与缩容操作，且同一中央控制器可统一纳管并调度不同 CPU 核心数、不同内存容量规格的异构流量调度引擎实例，实现资源的精准匹配与高效利用。

**2.HTTP 缓存加速：**

内置高性能 HTTP 内容缓存模块，采用内存 + 磁盘两级缓存架构，可智能缓存静态网页、图片、视频等 HTTP 内容，显著加快客户端页面加载速度，减少重复请求对后端业务服务器的访问压力，提升用户访问体验并节省服务器资源。

**3.优先级转发：**

支持 Pool Group 配置功能，可在 Pool Group 中创建多个 Server Pool 并为其分配不同的转发优先级，流量会优先转发至最高优先级的 Server Pool，当该 Pool 出现故障或负载过高时，系统会自动将流量平滑切换至次高优先级的 Pool，实现基于优先级的智能流量转发与业务容灾。

**4.应用性能监控：**

具备完善的应用性能监控功能，能够实时采集并记录从客户端到服务器的全链路性能数据，包括 TCP 连接时间、SSL 握手时间、首字节响应时间等核心指标，同时支持网络事件全量记录与按需回放功能，可重现任意时刻的网络流量与应用行为，帮助快速定位与排查网络故障。

**5.弹性扩缩容：**

支持自动化弹性扩缩智能流量调度引擎，能够根据实时网络流量、服务器负载等多维度指标自动触发流量调度引擎的扩容与缩容操作，且同一中央控制器可统一纳管并调度不同 CPU 核心数、不同内存容量规格的异构流量调度引擎实例，实现资源的精准匹配与高效利用。

**6.分布式架构：**

采用业界领先的管理平面与数据平面完全分离的分布式部署架构，实现了控制逻辑与数据转发的彻底解耦，支持多级故障域隔离，单个节点或区域故障不会影响全局业务运行，同时具备系统高可用性与弹性扩展能力，可根据业务需求平滑扩展集群规模。

**7.跨云智能流量调度：**

支持企业级跨云智能流量调度，原生集成 SSL Termination、全局智能流量调度（GSLB）与权威 DNS 服务，构建统一的跨云流量入口与安全加速平台。其中SSL Termination采用基于 Cavium Nitron V 的专用 ASIC 芯片 SSL 加速器，可提供最高 100Gbps 全 SSL 处理能力及 300K P256 ECC/OPS SEC 性能，将后端服务器的 SSL/TLS 加解密运算完全卸载至专用硬件执行，支持 SSL 卸载与 SSL 桥接双模式、TLS/SSL 协议自动转换、SNI 多域名证书、HSTS 安全增强及自定义加密套件，实现单虚拟服务最多 256 个证书的统一管理，大幅减轻后端服务器计算负担；全局智能流量调度（GSLB） 支持与 Luccitech 智能流量调度（SLB）深度无缝集成，可实现同设备或跨设备灵活部署，能够跨数据中心、跨云环境弹性扩展，采用远程 ADC 探针机制实时复用 SLB 虚拟服务器（VS）的运行状况检查能力，使 GSLB DNS 记录的运行状态与后端 SLB 节点的实际健康度精准联动，支持双活 / 多活集群部署模式及轮询等多种调度算法，基于用户地理位置、链路时延、节点负载等多维度将流量智能导向最优节点，实现跨地域业务高可用与用户就近访问；权威 DNS 服务作为跨云流量的基础寻址核心，负责将用户域名解析为最优业务节点 IP，与 GSLB 深度协同提供智能解析调度能力，是整个跨云智能流量调度体系的统一访问入口纽带。

## 十、安全与扩展性

**1.传输层安全加固：**

全面支持 TLS 1.0/1.1/1.2/1.3 等主流 TLS 协议版本，同时兼容 NIST 系列 (P-256、P-384、P-521) 与 Curve25519/X25519 等多种 ECDHE 椭圆曲线密钥交换算法，提供完美前向保密能力，支持灵活配置加密套件优先级列表，禁用不安全加密算法，实现传输层安全加固。

**2.视频业务弹性扩展：**

针对视频类业务提供专属智能流量调度解决方案，支持流量调度实例的分布式边缘部署，可根据视频业务流量的实时变化自动进行横向扩展，实现视频业务的弹性扩容与带宽资源的动态适配，有效应对视频流量的突发增长，保障视频播放的流畅性。

**3.OpenStack 生态集成：**

支持与 Mitaka、Newton、Ocata、Pike、Queens 等多个主流版本的 OpenStack 平台无缝集成，完全兼容 OpenStack Neutron LBaaS v2 与 Octavia 负载均衡服务标准 API，提供标准的 Octavia Provider Driver，可与 OpenStack 生态的认证、计算、网络、存储等服务深度对接。

## 十一、性能指标

**1.吞吐量：**

单套智能流量调度系统具备卓越的转发性能，4 层吞吐量可达 10Gbps，能够高效处理 TCP/UDP 等四层流量转发需求；7 层吞吐量可达 8Gbps，可满足 HTTP/HTTPS 等七层应用的高并发流量处理要求。

**2.连接数：**

单套智能流量调度系统支持最大 132000 个并发 TCP 连接，能够同时承载海量用户的业务访问请求，支持长连接与短连接混合场景，具备完善的连接超时管理机制，有效防止连接泄漏，保障系统稳定运行。

| **LCV 1088** | |
|---|---|
| **吞吐量（L4/L7）** | 10.8Gbps/10Gbps |
| **SSL TPS（2k密钥）** | 10,000 |
| **并发连接** | 35,000,000 |
| **七层最大并发数** | 262,500 |
| **四层每秒链接数** | 450,000 |
| **四层每秒请求处理** | 800,000 |
| **七层HTTP 每秒请求处理** | 175,000 |

## 十二、高可用与负载均衡

**1.多维度流量调度：**

提供多维度智能流量调度功能，支持基于 HTTP、HTTPS、四层端口、DNS 以及七层应用特征的流量调度策略，可根据不同业务需求灵活配置调度规则，实现精细化的流量管理与业务分流。

**2.集群高可用：**

支持 active/standby 主备、active/active 双活以及 active/active N+M 等多种集群高可用部署模式，采用 VRRP 协议与会话同步技术，实现秒级故障自动切换，切换过程中业务连接不中断，保障业务的连续稳定运行。

**3.安全负载均衡：**

通过多重技术手段保障负载均衡流量的加密传输安全，全面支持 TLS 协议实现数据传输加密，提供基于 Lua 语言的 DataScript 自定义脚本功能实现灵活的安全控制策略，同时支持 Consistent Hash 一致性哈希算法保障会话持久性与数据一致性。

## 十三、公司介绍

鸬鹚科技，拥有十余年的专业交付和安全产品经验，国内首家云应用交付产品解决方案前沿技术厂商。

团队名取自在中国常被寓意勤劳美好之鸟的鸬鹚，秉承 IT 服务精神。以帮助传统企业实现互联网+为己任，帮助国内外企事业实现跨越式安全 IT 构架，提供全球化 IT 支持方案的专业信息化产品，目标成为国外 F5 和 Citrix 等同类专业 IT 增值领军厂商。

鸬鹚科鸬鹚科技致力于通过云应用交付平台为整体解决方案，为行业企业客户提供有前瞻性、云演进性的专家级行业应用交付服务，迄今已为中国多家行业信息化领军企业提供整体交付方案和服务，以帮助中国企业提供全球化 IT 支持方案的领军企业为目标的专业信息化产品公司。

我们立足世界最前沿、最具前瞻性技术的本地化研发和服务，公司拥有的专业云应用交付产品、行业混合云交付平台（含云灾备、云负载集群管理、企业自建 CDN、IPv6 改造等专业服务）、应用负载均衡、全局负载均衡、链路负载均衡产品、云负载均衡等一系列可以与国际同步的专业产品和解决方案，正在大型国企信息化优化业务、国内互联网金融、金融保障、智慧智慧政务、智慧医疗智慧旅游、智慧法务、智慧教育、智慧财政等传统的政企客户和互联网+的专业客户的环境中使用并实现国产化产品替代和方案的落地，同时我们和广大的私有云平台商（VMware、MicrosoftHyper-V、CitrixXen、OracleVirtualbox、各类的基于 KVM 的私有云平台商等）、公有云服务商（MicrosoftAzure、华为云、腾讯云、阿里云
等）、云 IDC、云应用开发商、服务器厂商、各类行业系统集成商等合作方案中陆续落地。队名取自在中国常被寓意勤劳美好之鸟，鸬鹚，秉承 IT 服务精神。以成为帮助传统企业实现互联网+，帮助国内外企事业实现跨越式安全 IT 构架，提供全球化 IT 支持方案的专业信息化产品领军企业。拥有上百家省级和典型用户，品牌快速成长，目前拥有国内最专业的云应用交付团队

适配华为、微软、Vmware、AWS、阿里、腾讯等专业云生态优势。

我们的高附加值解决方案能够能够帮助国内企业提升产业信息化能力能力，通过国产化替代，降低对国外相关高附加值产品的依赖。

产品起点高、专业、拥有核心技术产品和国内定制开发能力，基于多云的安全、快速、智能为目标设计的产品，具备高性能 ASIC 级硬件、私有云、公有云三种交付方式。全面支持各种云环境升级改造，支持技术融合，桌面应用交付更简单，提供各种国内外应用集群架构优化加速方案、混合云架构支持、灾备方案优化、IPv6 改造支持、传统 VDI 架构改造升级支持，各种应用端和外设适配方案，并为未来的 AI 云引擎和自动化运维做准备，我的解决方案既支持龙芯等国产化硬件，国内各种软件环境，各种云、各种网络适应。

作为国内自主开发的专业应用交付（中间件）软件及硬件，能够有效连接

NetOps 与 DevOps, 为用户提供基于全环境的统一应用服务。从比较宏观的角度上看，通过引入 Luccitech 应用安全性和丰富应用服务组合，加上领先的云应用交付虚拟化版和 丰富的 API 管理（380 多个 API） 解决方案，将在所有环境中实现多云应用服务，提供开发人员所需的易用性和灵活性，同时还提供网络运营团队所需的规模、安全性和可靠性。并能提供更具专业性的 敏捷开发解决方案， 帮助开发实践更加多元化，并有扮演着智能流量调度的角色。 鸿鹕云应用交付产品短短 4 年多时间，实现以下的突破：

1、相关技术水平国内领先，并保持和国际理念同步。

2、成功交付 100+以上客户（包括广东省高院、广东省教育厅江西省工信委等省级单位， 中国机械设备工程有限公司等国家级企业以及广州番禺何贤医院、南昌第一人民医院等 医疗教育机构等）

3、016-2019 年连续三年广东省计算机用户推荐产品奖

4、2018 年中国云应用交付用户最值得信赖产品奖

5、深圳市双软企业

6、深圳市信息技术应用创新联盟发起单位

7、2018 年获得华为云等公有云认证，成为国内支持公有云和私有云最多的专业云应用交 付器厂商。

8、2018 年广东省计算机用户协会副会长单位/前海云计算及人工智能产业联盟会长单位

9、2019 年入围腾讯云数字广东合作企业/入围全国联通数字医院解决方案和产品合作企 业

10、 2019 年团队项目入选阿里云 AI 赛道明星企业

11、 2019 年鸿鹕杯华东交通大学“交通智能网创新创业”大赛支持团队

12、 2019 年全国创新大赛百度赛区半决赛

13、2019 年全球名校创业创投（南京）大赛 总决赛优秀奖（前十二强）

14、2019 年鸿鹕科技正式成为国家级高新企业