a Hewlett Packard Enterprise company

结合 AC+CPPM 来实现外置的 Radius-based 认证源和本地 Endpoint DB 的主备切换

2021 年 8 月

目录

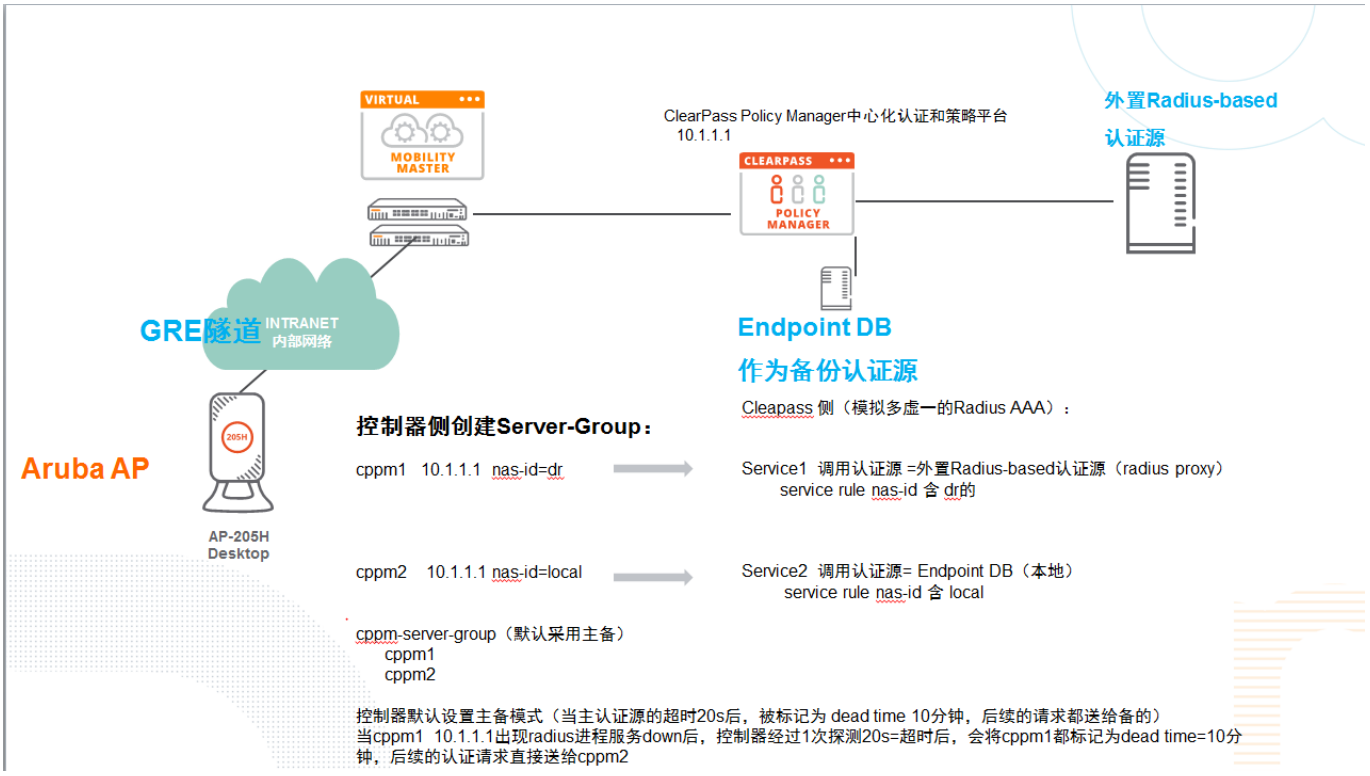
1 背景描述

CPPM 作为 AAA Server 提供了 Radius 协议认证，同时在一个认证 Service 中可以调用多个外置的认证源（Radius-Based，SQL，LDAP，AD 等等），可以针对多个外置认证源实现账号的轮询查询，例如到第一个认证源查询账号，如果查询不到会继续到第二个认证源查询，直到找到账号且密码正确，则认证成功。找到账号且密码错误，则认证失败，如果一直找不到账号，则最终还是认证失败。

2 原因

但是 CPPM 上单一的认证 Servcie 中的多个认证源并不都是按照从上到下的顺利来轮询账号的，如果我们在一个认证服务中调用多个认证源，Radius-based 的认证源在前，而本地或者外置的 SQL 数据库/外置的 LDAP/外置 AD 类型的认证源在后，或者调用多个 Radius-based 的认证源时，即使第一个 Radius-based 的认证源查询不到指定账号或者故障 down 了，那么 CPPM 也是无法实现账号轮询和认证源的主备切换功能的。所有的认证请求仅在第一个 Radius-based 的认证源中查询，即使账号找不到或者第一个认证源无响应了，CPPM 也不去第二个认证源中查询。
那如何解决采用 Radius-based 的认证源在前，而本地或者外置的 SQL 数据库/LDAP/AD 类型的认证源在后，或者调用多个 Radius-based 的认证源时，需要实现账号轮询或者主备切换呢?

3 解决方法



我们利用 AC+CPPM 作为解决方法，在 AC 上创建 Server Group，采用默认的主备模式，里面调用两个 Radius 类型的认证服务器 CPPM1 和 CPPM2，IP 地址都指向到 CPPM，通过设置不同的 NAS ID 来区分两台 Radius 类型的认证服务器。在 CPPM 上，创建两个认证 Service，通过 Service Rule 来匹配来自不同 CPPM1 和 CPPM2 的认证请求。同时在这两个认证 Service 中，各自分别调用各自的认证源，Service1 调用的认证源是外置的 Radius-based 的认证源，Service2 调用的认证源是本地的 Endpoint DB（SQL 类型的）。正常的用户认证请求到达 AC，然后 AC 将所有的认证请求都发给第一台认证服务器 cppm1 来认证。有认证成功的（账号和密码都正确），有认证失败的（账号正确，但密码错误），有查不到账号的，最终也是认证失败。当 cppm1 （其实就是后台的外置 Radius-based 的认证源）故障 down 了或者无响应了，那么控制器会将认证请求发给第二台认证服务器 cppm2 来认证， 并标记第一台 cppm1 dead time =10 分钟，在这 10 分钟的时间内，AC 会将后续的认证请求直接发给 cppm2. 后续的认证请求直接转发给 cppm2 后，如果账号和密码正确，则认证过，如果账号在，密码错误，则认证失败， 如果账号查不到，则最终认证失败，因为已经是这个 Server-Group 中的最后一台认证服务器了。

10 分钟后，AC 会尝试重新和 cppm1 建立通讯。

附录：提供 CPPM 上单个 service 下，如果调用了多个认证源时，认证顺序如何?

A:多个认证源（**如果是多个相同 SQL 数据库类型的认证源或者多个相同 AD 类型的认证源**）起**到冗余备份和账号轮询的作用**，但是没有 fail-through（认证失败后的轮询）功能

认证顺序：

1）认证请求先到第一个认证源中查询，如果找到账号且密码正确，则认证成功。如果找到账号且密码错误，则认证失败；此时不会再继续向第二个认证服务器中进行查询。

如果第一台**认证源中查不到用户账号/第一台认证源无响应超时，**那么认证请求会按照顺序，CPPM 自动会发送到第二个认证服务器上。

2）在第二个认证服务器上，找到账号且密码正确，则认证成功。如果找到账号且密码不正确，则认证失败。此时不会继续向第三个认证服务器中进行查询。如果第二台认证服务器查不到账号/第二台认证源无响应超时，那么认证请求会按照顺序发送到第三个认证服务器上。依次类推。

B：多个认证源（**如果是多个相同 Radius -based 类型的认证源**），**认证请求只到第一个认证源查询。**

认证顺序：

认证请求先到第一个认证源中查询，如果找到账号且密码正确，则认证成功。如果找到账号且密码不正确，则认证失败；如果第一个**认证源中查不到用户账号/ 第一个认证源无响应**

那么认证请求仍然发到第一个 radius -based 认证源，始终**不会发给第二个。**

也就是说，即使第一个 radius-based auth resource down 了或者无响应了，认证请求也不会到第二个去，所以调用多个 radius-based 类型认证源的认证 service 服务是没有意义的。

C:当 radius –based 类型的认证源和本地/外置 SQL 数据库/LDAP/AD 类型的认证源在同一个 service 中被调用时，radius–based 类型的认证源在前，本地/外置 SQL 数据库/LDAP/AD 类型的认证源在后，以 radius-based 认证源为优先的，不会到本地/外置 SQL 认证源来查询。

即使 radius–based 认证源无响应，也是仅到 radius -based 认证源为优先的。

认证顺序：
认证请求直接到 radius-based 中查询，如果找到账号且密码正确，则认证成功。如果找到账号且密码不正确，则认证失败；如果第一个**认证源中查不到用户账号/ 第一个认证源无响应，**那么认证请求仍然发到 radius-based 认证源，始终**不会发给其他的认证源。也就是说，即使 radius-based auth resource down 了或者无响应了，认证请求也不会到其他的去，**此时永远**不会再继续向第二个认证服务器中进行查询。**

D:当 radius –based 类型的认证源和本地/外置 SQL 数据库/LDAP/AD 类型的认证源在同一个 service 中被调用时，本地/外置 SQL 数据库/LDAP/AD 类型的认证源在前，radius –based 类型的认证源在后。

认证顺序：
认证请求先到本地/外置 SQL 数据库/LDAP/AD 类型的认证源中查询，如果找到账号且密码正确，则认证成功。如果找到账号且密码不正确，则认证失败；
如果第一个**认证源中查不到用户账号/ 第一个认证源 down 了或者无响应，**那么认证请求继续发到 radius-based 认证源继续查询和认证。