

什么是“认证逃生”(auth-survivability)?

AOS 8.6.0.0

fox210317@sina.com

2022/11/15

一、什么是 Auth survivability ?

- 该功能允许控制器在外部认证服务器宕机时，使用控制器提供身份验证与授权
- 该功能会通过控制器存储用户认证的凭证信息，以及外部认证服务器回应的属性
- 该功能仅能维护已通过认证用户的连接

二、它支持那种认证方式?

- Captive Portal: PAP
- EAP-Termination disable: 外置认证服务器 EAP-TLS
- EAP-Termination enable: 外置认证服务器 EAP-TLS with CN lookup
- External Captive Portal 使用 XML-API: PAP
- MAC 认证: PAP

三、Auth-Survivability 如何工作的

Auth-Survivability 可在控制器层级开启或关闭，默认关闭

关联的客户端通过认证时，两种类型的信息会被控制器存在本地 MySQL DB

- 1) Client access credential
- 2) Key reply attributes

除了客户端的 `username`，以下信息也需要存储：

- 对于 PAP 用户 `authmgr` 存储密码的加密 SHA-1 散列值
- 对于 EAP Termination disable 的用户，存储 EAP-TLS 指示符
- 对于 CN 查找的用户，存储 EXIST 指示符

存储信息的前提条件：

- 客户端 MAC Address 不能是全 0
- EAP-TLS 认证的客户端，Survival server certificate 需要预安装在客户端设备中，并作为 Trusted CA
- EAP Termination disable 的 EAP-TLS 认证的客户端，issuer cert 必须作为 Trusted CA 或者 Intermediate CA 导入控制器

Survival Server 在如下情况下开始对客户端进行身份验证

- 1) Survival Server 由一个 Free RADIUS Server 和 MySQL 数据库组成，它被配置为接受本地主机的 RADIUS Requests，并在 MySQL 中检索 credential 和 Key reply attributes.
 - 1.1. fail through disable、server group 中的所有 servers 均无法提供认证服务
 - 1.2. fail through enable、server group 中至少有一台服务器无法提供认证服务（OOS）
- 2) 所有缓存的 credential 和 Key reply attributes 会在缓存时间后失效，默认为 24h
- 3) 在如下情况下，缓存条目会从本地 Survival Server 中删除：
 - 3.1. fail through disable, 用户通过外部认证服务器认证失败

3.2. fail through enable, 用户使用 server group 中所有认证服务器认证均失

败

4) 每 10 分钟清除一次过期条目

四、配置

Parameter	Description	Default
cache-lifetime <hrs>	此参数指定本地 Survival Server 中缓存的访问凭据的生命周期（以小时为单位）。当指定的缓存生存期到期时，缓存的访问凭证将从 Survival Server 设备中删除。 有效范围为 1 到 72 小时。	24 hours
enable	该参数控制当 server group 中没有其他服务器处于服务状态时是否使用 Survival Server。该参数还控制当 server group 中有外部 RADIUS 或 LDAP 服务器认证时，是否将用户访问凭证存储在 Survival Server 中。在每台 MD 上启用或禁用此功能。 注意：如果身份验证服务器 dead time 配置为 0，auth-survivability 失效	Disabled
server-cert	该参数允许查看本地 Survival Server 使用的服务器证书的名称。本地 Survival Server 提供了来自 AOS 的默认服务器证书。必须先将客户服务器证书导入 MD，然后才能将服务器证书分配给本地 Survival Server。 注意：在部署环境中，建议切换到客户服务器证书。	-

网页配置截图

The screenshot shows the web configuration interface for a Mobility Controller. The left sidebar displays the navigation menu with 'Configuration' expanded. The main content area is titled 'Advanced' and shows the 'Survivability' configuration page. A red box highlights the following settings:

- Enable auth survivability:
- Auth server certificate:
- Local cache lifetime: Hour

Below these settings, there are expandable sections for 'Authentication Timers', 'RADIUS Client', 'TACACS Client', 'DNS Query Interval', and 'EAP Fragmentation IP MTU'.

命令行配置截图

```

Session Manager
WARNING: This system is for the use of authorized clients only.
Individuals using the computer network system without
authorization, or in excess of their authorization, are
subject to having all their activity on this computer
network system monitored and recorded by system
personnel. To protect the computer network system from
unauthorized use and to ensure the computer network systems
is functioning properly, system administrators monitor this
system. Anyone using this computer network system
expressly consents to such monitoring and is advised that
if such monitoring reveals possible conduct of criminal
activity, system personnel may provide the evidence of
such activity to law enforcement officers.
Access is restricted to authorized users only.
Unauthorized access is a violation of state and federal,
civil and criminal laws.

(7010) [mynode] #
(7010) [mynode] #configure terminal
Enter Configuration commands, one per line. End with CNTL/Z

(7010) [mynode] (config) #aaa auth-survivability
cache-lifetime      lifetime of cached credential for survival server
enable              Enable Auth Survivability
server-cert         Server Certificate for Survival Server

(7010) [mynode] (config) #aaa auth-survivability

```

五、验证

```
#show aaa auth-survivability
```

```
Auth-Survivability: Enabled (Running)
```

```
Survival-Server Server-Cert: server-cert
```

```
Survival-Server Cache lifetime: 24 hours
```

```
# show aaa auth-survivability-cache
```

```
Auth-Survivability Cached Data
```

```
-----
```

```
Station          User Name          Authenticated Using  Authenticated By
Authenticated On
```

