BYO局域网开机认证用户手册

V 1.0

目录

[BYO局域网开机认证用户手册 1](#_Toc131080514)

[1.功能介绍 3](#_Toc131080515)

[1.1功能描述 3](#_Toc131080516)

[1.2认证场景 3](#_Toc131080517)

[1.3密码状态 3](#_Toc131080518)

[2.工作原理 5](#_Toc131080519)

[3.硬盘密码网络认证 6](#_Toc131080520)

[3.1客户端网络标识注册 6](#_Toc131080521)

[3.2获取网络标识的时间点 6](#_Toc131080522)

[3.3网络认证功能开关 6](#_Toc131080523)

[3.4密码验证以及网络认证重试次数 7](#_Toc131080524)

[4.ByoNetworkIdTool 8](#_Toc131080525)

[4.1工具简介 8](#_Toc131080526)

[4.2功能描述 8](#_Toc131080527)

[4.3使用方法： 8](#_Toc131080528)

[参考文档 9](#_Toc131080529)

# 1.功能介绍

## 1.1功能描述

1. 客户端在注册某个局域网络后（如 公司内网，财务内网，家庭内网等），启动网络围栏功能；
2. 其后固件启动过程中，客户端只有连接到注册的网络中，才能进行用户密码验证；
3. 如客户端没有处于注册网络中，则即使用户输入正确密码也不能通过验证；

**注：S3 Resume场景下仅需自动解锁，不需要网络验证，因此不需要手动操作。**



## 1.2认证场景

在系统设计中，系统固件由于自身特性，通常被赋予平台所有者(Platform Owner)的角色。如需修改系统配置，或访问敏感信息，用户必须提供密码（Password），由系统固件验证身份后才能获得对应权限。以下是部分使用密码的场景:

|  |  |
| --- | --- |
| 密码 | 对应权限 |
| 系统User/Admin Password | 进入Setup配置  BIOS系统工具修改配置 |
| 安全存储设备密码 | ATA/OPAL/OPALite/OPALPyrite（Specific Device） 安全存储设备解锁 |

## 1.3密码状态

* 密码部署

1. 系统或设备初始状态为解锁状态；
2. 用户启用密码（管理员密码/用户密码）；
3. 系统密码重启后安全状态更新为锁定，硬盘设备则需冷重启后才能更新为锁定状态，（ATA\_SEC的NVMe除外）。

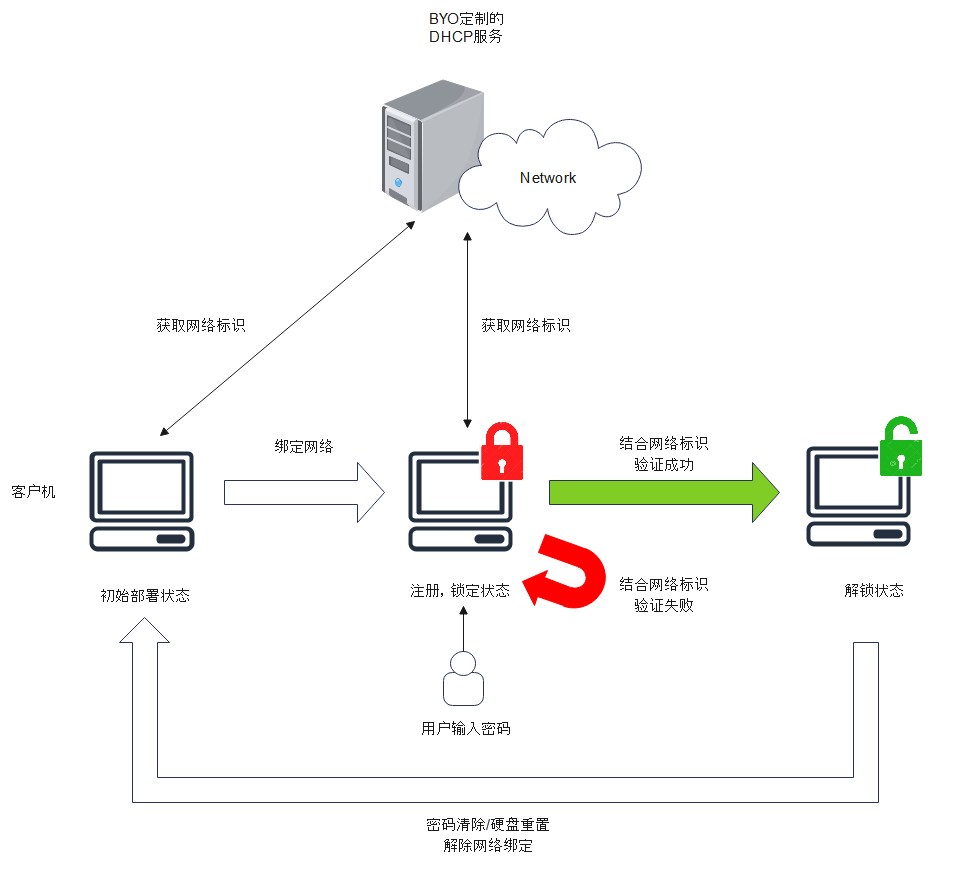
* 密码验证

1. 系统或设备状态为锁定。
2. 用户输入管理员/用户 密码进行密码权限认证;
3. 如果密码验证通过，则系统或设备安全状态跟新为解锁，用户获得相应设备/系统使用权限（管理员权限/用户权限）。否则仍保持锁定

* 密码清除

系统或设备处于解锁状态后，可通过密码禁用选项禁用密码管理功能

# 2.工作原理



# 3.硬盘密码网络认证

## 3.1客户端网络标识注册

1. 客户端启用此功能前需用Byo工具ByoNetworkIdTool在当前局域网Sever中注册NetworkId（当前工具仅支持Linux Server）
2. ByoNetworkIdTool功能包含：NetworkId部署、NetworkId更新
3. 注册之后同一局域网内所有Sever应被同一NetworkID唯一标识

（[ByoNetworkIdTool](#_4.ByoNetworkIdTool)）

## 3.2获取网络标识的时间点

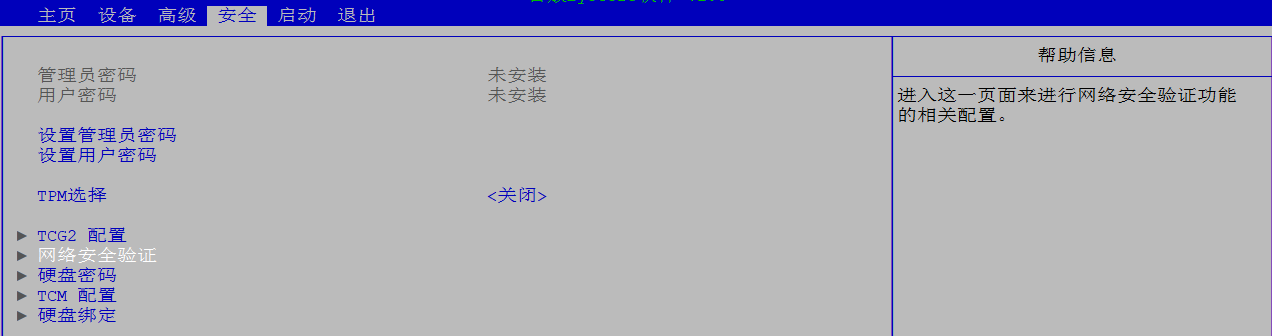
为保证网络标识的时效性，每次验证用户密码前都需要重新获取网络标识，确保设备连接在已经注册绑定的网络中。

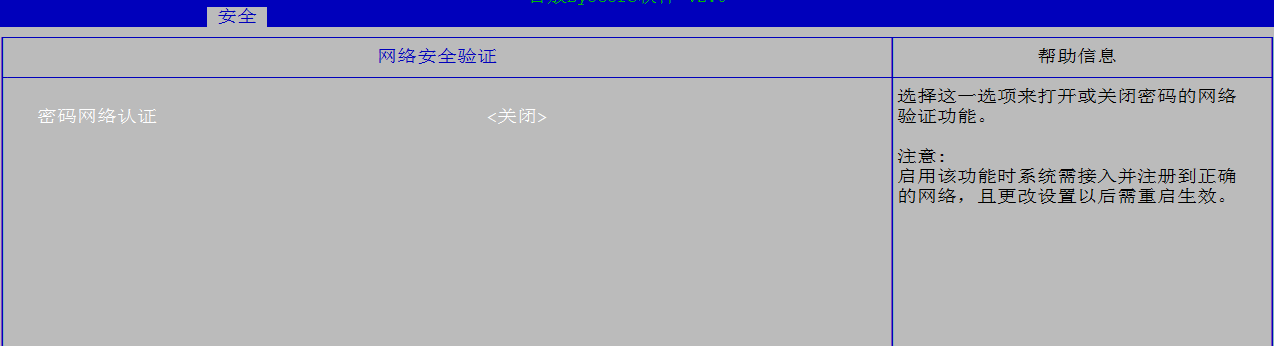
如果有多个处于已加密、未解锁状态的硬盘设备，启动到POST阶段时，进行密码验证之前先进行一次获取网络标识总验证，成功之后再进行逐一验证。此阶段只显示总验证，单一解锁时不提示信息。

## 3.3网络认证功能开关

1.系统密码与硬盘密码网络认证功能均需通过密码网络认证功能打开，且重启后生效。

2.选项如图所示





## 3.4密码验证以及网络认证重试次数

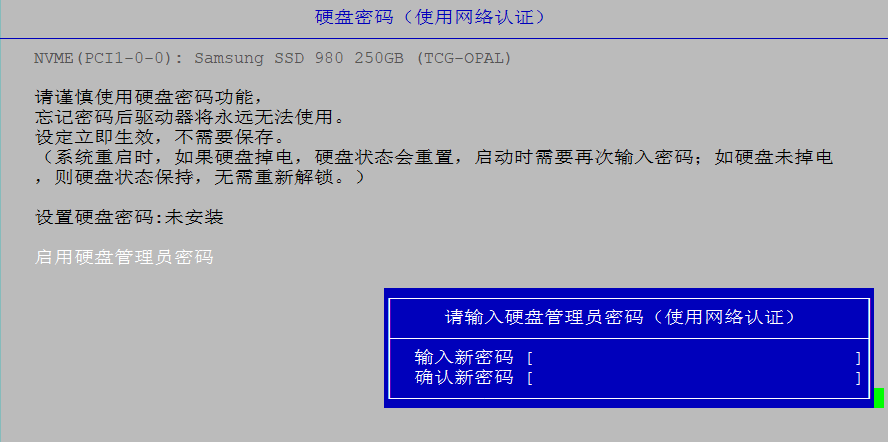
1.密码验证次以及行为同启用网络认证功能前

2.网络认证在每次密码验证前，如果网络认证失败则RetryCount++,上限为三次，如果三次重试中有一次成功，测RetryCount清0；

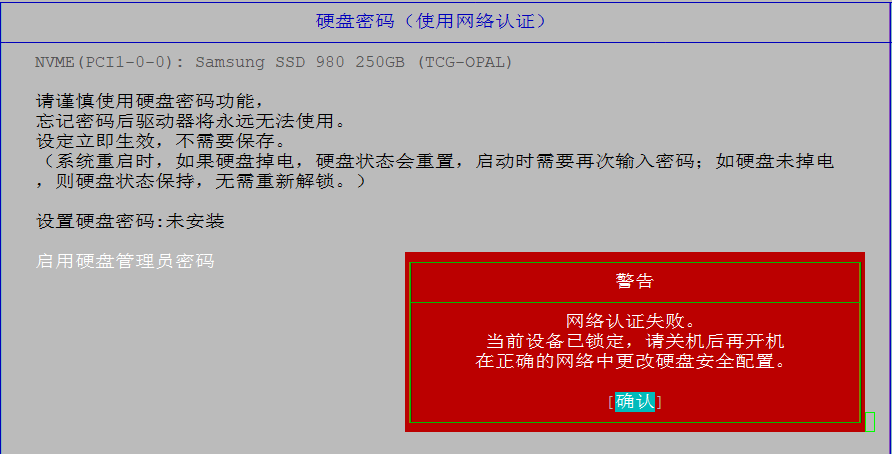
3.如果网络认证连续三次重试均失败，则停止所有密码验证功能。系统重启后重置RetryCount == 0；

（注意：当前网络认证的重试机制为内部程序执行中实现，显示接口并未直观提示每次重试）

硬盘密码网络认证成功：



硬盘密码网络认证失败：



# 4.ByoNetworkIdTool

## 4.1工具简介

1. ByoNetworkId工具用于部署局域网DHCP服务器（Linux）网络标识（NetworkId）。实现网络围栏功能。

## 4.2命令介绍

|  |  |
| --- | --- |
| 命令 | 说明 |
| python3 ByoNetworkId.py | 自动部署模式，手动输入dhcpd.conf路径，自动生成UUID, 更新dhcpd.conf |
| python3 ByoNetworkId.py -u <UUID> | 手动部署模式，手动输入dhcpd.conf路径,用户输入UUID, 更新dhcpd.conf |
| python3 ByoNetworkId.py -h | 查看帮助信息 |
| python3 ByoNetworkId.py -f <file path> | 两种部署模式都需要使用-f 输入dhcpd.conf文件路径,以便在其他目录下也可以进行部署 |

## 4.3ByoNetworkId部署流程

### 单台DHCP服务器处理

1 . 运行sudo systemctl stop dhcpd 暂停dhcp服务

2. 自动部署模式生成一个32位的UUID，作为局域网NetworkId

3. 或手动部署模式，由用户手动输入UUID，作为局域网NetworkId

4. 运行sudo system start dhcpd 重新启动dhcp服务

### 同一局域网内存在多台DHCP服务器的处理

需要使用手动输入模式，保证所有DHCP服务器使用同一NetworkId。可首先选择一台DHCP服务器上使用自动模式部署，并记录下32位的UUID，在其他DHCP服务器中输入这个被记录的UUID，完成整个局域网的NetworkId更新。

### 出错恢复

部署过程中，原有dhcpd.conf文件会自动备份到相同目录下dhcpd\_backup.conf文件。 如果出现预期之外的错误，可使用此备份文件进行恢复。

# 参考文档

[1]BYO系统保护与安全网络认证-方案设计