关于iMC操作员登录控制的典型配置

PLAT 何颖 2013-04-23 发表

关于iMC操作员登录控制的典型配置

一、 组网需求：

使用iMC产品的配置前台，需要先使用操作员登录进入管理前台，然后才能执行各种业务功能和操作。

二、 组网图：

实际参考iMC服务器的部署组网即可。

三、 配置步骤：

iMC操作员登录控制特性提供如下管理手段：

1) 不同的认证方式：操作员可以使用iMC内嵌的操作员管理功能对操作员进行认证，也可以与RADIUS或LDAP服务器联动实现操作员的身份认证。

2) 登录地址控制：iMC可以控制客户端的登录地址，只允许用户从特定的地址（范围）登录iMC。

3) 密码控制策略：如果操作员在iMC系统上进行密码认证，则可以控制密码的强度、失效日期等。

4) 密码防破解：iMC可以有效防范通过连续尝试的方式破解密码的非法行为。

l iMC管理员可使用不同的登录认证方式。iMC提供三种操作员登录认证方式：

1) 简单密码认证：使用iMC系统数据库中存放的操作员密码进行身份认证，是最常用的身份认证方式。

2) RADIUS认证：使用iMC特定操作员的“操作员登录名”或“操作员全称”作为用户名，以及用户在登录时输入的密码，到RADIUS服务器进行身份认证。

3) LDAP认证：使用iMC特定操作员的“操作员登录名”或“操作员全称”作为用户名，以及用户在登录时输入的密码，到LDAP服务器进行身份认证。

通过如下步骤，可配置不同的登录认证方式：

步骤一：配置操作员的登录认证方式。在增加或修改操作员界面，选择“登录认证方式”中的一种。如果选择了“简单密码认证”，则必须输入“登录密码”和“登录密码确认”；如果选择了“RADIUS认证”或“LDAP认证”，则无需输入登录密码信息。参考界面如下：

图1-1 配置登录认证方式

步骤二：如果使用“RADIUS认证”或“LDAP认证”，则同时需要对认证服务器进行配置。使用iMC的管理员登录iMC配置台，在“系统管理”中，点击“认证服务器配置”，根据需要对RADIUS认证服务器或LDAP认证服务器进行配置。参考界面如下：

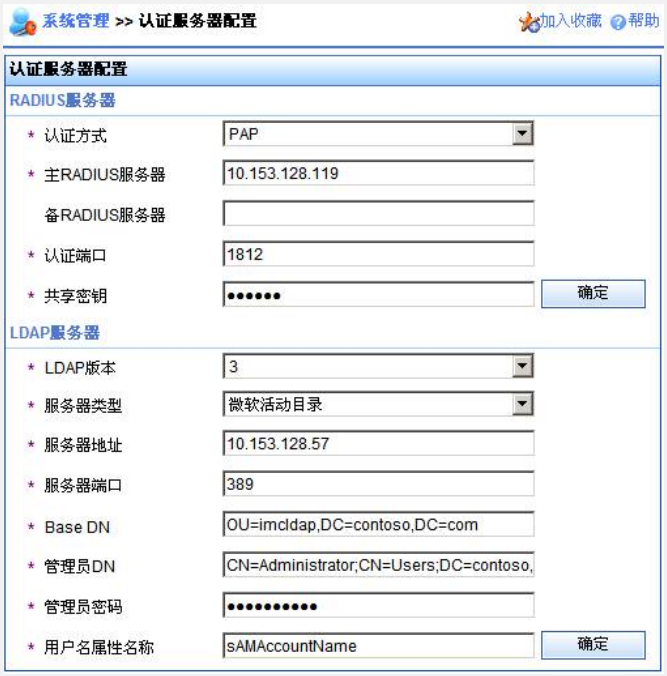

图1-2 认证服务器配置界面

目前支持的RADIUS认证方式包括“PAP”和“CHAP”两种；支持的LDAP版本包括2和3两个版本；支持的服务器类型包括“通用LDAP服务器”和“微软活动目录”两类。用户可根据需要进行配置，各参数的详细说明可参考联机帮助。

l 登录地址控制。

iMC允许控制用户的登录客户端地址，即允许或禁止从某些地址（范围）登录。

在增加或修改操作员时，在“操作员访问控制列表”部分进行配置，如下图所示：

图1-3 登录地址控制的配置界面

上图的配置，只允许该操作员从“192.168.0.1-192.168.0.255”和“192.168.1.1-192.168.1.255”两个地址区域进行登录。

iMC操作员访问控制列表的匹配策略为“首先命中匹配”。例如：假设同时配置了“允许”地址段和“禁止”地址段，则在操作员进行登录时，将客户端的IP地址按照访问控制列表的顺序从上到下逐行匹配，如果与某段地址匹配成功，则使用该段地址的“访问类型”进行控制，即如果“访问类型”为“允许”，则允许登录；反之则禁止登录。如果所有地址段均不匹配，则使用“缺省访问控制列表匹配策略”的配置值进行控制。

此外，为了增加地址段的可重用性，iMC系统还提供了“访问控制模板”配置功能。在配置特定操作员的访问控制列表时，可以直接从已经配置好的模板中选取。

l 密码控制策略。

iMC系统提供密码控制策略的配置，用于对操作员的登录密码管理进行监控。密码控制策略为全局配置，即对所有认证方式为“简单密码认证”的操作员均有效。如果操作员的认证方式为“RADIUS认证”或“LDAP认证”，则密码控制策略对该操作员无效。

使用iMC的管理员登录iMC配置台，在“系统管理”中，找到“密码控制策略”，点击进入如下配置界面：

图1-4 密码控制策略配置界面

各个参数的含义较明确，不再赘述。

l 密码防破解。

当使用某个操作员在同一个客户端连续尝试执行三次登录操作，且均失败时，iMC系统将在一分钟内禁止在该客户端上使用相同操作员继续执行登录操作（锁定）。一分钟后可以尝试一次，如果还是失败，则继续锁定一分钟。

需要注意的是：“失败”的原因不仅是密码错误，如果访问控制列表禁止或认证服务器不可用，均会登录失败，这些失败情况均用于密码防破解策略的判断条件。

该策略缺省启用，不允许关闭。

四、 **配置关键点：**

使用RADIUS认证和LDAP认证时，需注意：

1） 采用RADIUS或LDAP认证方式时，应使用“操作员登录名”或“操作员全称”作为RADIUS或LDAP身份认证的用户。即在RADIUS或LDAP身份认证时，首先尝试使用“操作员登录名+密码”进行认证；如果失败，则尝试使用“操作员全称+密码”进行认证。只要任何一种方式认证成功，则能成功登录。

2） 当iMC的所有操作员（包括超级管理员“admin”）均使用RADIUS或LDAP方式进行身份认证时，如果由于意外故障导致RADIUS和LDAP服务器不可用，则无法再登录iMC。此时可以通过密码重置工具脚本（iMC安装路径\client\bin\resetpwd.bat），将操作员的认证方式和密码重置为缺省值（简单密码认证，缺省密码为“admin”）。