目录

简介

本文在验证提供信息在统一通信管理套件(UCSM)和步骤的轻量级目录访问协议(LDAP)配置调查LDAP认证失败问题。

配置指南：

[配置验证的UCSM](#)

[示例激活目录(AD)配置](#)

验证UCSM IDAP配置

确保UCSM通过检查有限状态机(FSM)状态成功部署配置，并且显示完成在100%。

从UCSM命令行界面(CLI)上下文

从连结操作系统的(NX-OS) CLI上下文

IDAP配置最佳实践

1. 创建另外的验证域而不是更改"本地Authenitcation"领域

2. 总是请使用本地范围'控制台验证'，万一用户从使用'本地验证'锁定， admin能从控制台访问它。

3. UCSM总是失效回到本地认证，如果在给的验证域的所有服务器失败回应在登录尝试期间(不可适用为aaa命令的测验)。

验证IDAP配置

使用NX-OS命令，测试LDAP认证。'测验aaa'命令从NX-OS CLI接口是仅可得到。

1. 验证LDAP基团特殊性的配置。

以下命令通过根据他们的配置的顺序的所有已配置的LDAP服务器列表。

2. 验证特定LDAP服务器配置

注意：<password>字符串在终端将显示。

在这种情况下，如果没有为指定的LDAP服务器，配置的过滤器UCSM测试验证特定服务器，并且可以发生故障。

排除故障LDAP登录失败

此部分在诊断提供信息LDAP认证问题。

问题场景#1 -不能登陆

不能登陆作为LDAP用户通过UCSM图形用户界面(GUI)和CLI

收到**"错误验证对服务器的"**用户，当测试LDAP认证时。

建议
由互联网控制消息协议(ICMP) ping验证LDAP服务器和结构互连(FI)管理接口之间的网络连通性和从本地mgmt上下文的设立Telnet连接

如果UCSM不能ping LDAP服务器或开始远程登录会话到LDAP服务器，请调查网络协议(IP)网络连通性。

请验证，如果域名服务器(DNS)回归更正IP地址对LDAP服务器主机名的UCS并且确保， LDAP流量没有阻塞在这两个设备之间。

问题场景#2 -登录GUI，不能登录SSH

LDAP用户通过UCSM GUI登录，但是不能开始SSH会话到FI。

建议

当建立SSH会话对FI作为LDAP用户时， UCSM要求“在LDAP前”将被加在前面的ucs- domain-name

*从Linux/MAC计算机

*从PuTTY客户端

注意：*域名区分大小写，并且应该匹配domain-name已配置的在UCSM。包括域名的最大用户名长度可以是32个字符。*

“ucs-<domain-name> \ <user name>” = 32个字符。

问题场景#3 -用户有只读权限

LDAP用户能登陆，但是有只读权限，即使LDAP组地图在UCSM正确地配置。

建议
如果角色未在LDAP登录过程中获取，远程用户允许与默认角色(只读访问)或拒绝访问(NO-洛金)登录到UCSM，根据远程登记策略。

当用户登录和用户给只读访问，在那种情况下请验证在LDAP/AD的用户组会员详细信息。
例如，我们能使用ADSIEdit程序MS活动目录。或者在Linux/Mac的情况下ldapserach。

它可能用“从NX-OS shell的测验aaa”命令也验证。

问题场景#4 -不能登陆与‘远程验证’

用户不能登录也不访问只读访问UCSM作为远程用户，当“本地验证”更改到远程验证机制(LDAP等)

建议
作为对本地认证的UCSM fallsback控制台访问的，当不能到达远程验证服务器时，我们能在步骤之下跟随恢复它。

1. 断开主要的FI mgmt接口电缆(show cluster状态会指示哪些作为主要的)
2. 连接到主要的FI的控制台
3. 执行跟随的命令更改本地验证

4. 连接mgmt接口电缆
5. 通过UCSM登陆使用本地帐户并且创建远程验证(前LDAP)组的验证域。

注意：*断开mgmt接口不会影响任何数据层面流量。*

问题场景#4 - LDAP认证，但是不与启用的SSL一起使用

当SSL选项启用时， LDAP认证优良工作，不用安全套接字层SSL，但是发生故障。

建议
UCSM LDAP客户端使用已配置的托拉斯点(Certificate Authority (CA)证书)，当建立SSL连接时。

1. 确保托拉斯点正确地配置。

2. cert的识别字段应该是“主机名“LDAP服务器。确保在UCSM配置的主机名匹配主机名现在证书并且有效。

3. 确保UCSM配置与‘’不是‘主机名IP地址’的LDAP服务器，并且从本地mgmt接口是recheable。

问题场景#5 -，在LDAP供应商更改后，验证发生故障

验证在删除旧有LDAP服务器和添加新建的LDAP服务器以后失效

建议
当LDAP时用于验证领域，删除和添加新的服务器没有允许。从UCSM 2.1版本，它将导致FSM失败。

跟随的步骤，当删除/添加在同样处理的新建的服务器是

1. 确保所有验证领域使用ldap更改对本地并且保存配置。
2. 更新LDAP服务器并且验证FSM状态顺利地完成。
3. 更改在step1修改的域验证领域，成LDAP。

其他问题场景-调试LDAP

打开调试，尝试登陆作为LDAP用户和采集根据日志与失败的捕获登陆事件的UCSM techsupport一起。

1) 开始SSH会话对FI并且登陆作为本地用户并且变成NX-OS CLI上下文。

2) 启用跟随的调试标志并且救SSH会话输出到日志文件。

3) 现在请开始一新的GUI或CLI会话并且尝试登陆作为远程(LDAP)用户
4) 一旦已接收登录失败消息，**关闭调试。**

LDAP流量数据包caputure

在数据包捕获要求的方案， Ethanalyzer请能过去常常捕获FI和LDAP服务器之间的LDAP流量。

在上述命令， pcap文件保存在/workspace/diagnostics目录下，并且可以从FI获取通过本地mgmt CLI上下文

在命令上能使用获取所有远程(LDAP， TACACS， RADIUS) authenitcation流量的数据包。
5. 相关登录UCSM techsupport套件

在UCSM techsupport，相关日志查找在**<FI>/var/sysmgr/sam_logs目录下**

已知问题说明

CSCth96721
LDAP服务器rootdn在山姆的应该允许超过128个字符

UCSM的版本早于2.1有127个字符的限制基础DN/捆绑DN字符串的。

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/cli/config/guide/2.0/b_UCSM_CLI_Configuration_Guide_2_0_chapter_0111.html#task_0FC4E8245C6D4A64B5A1F575DAEC6127

---------截取----------
在服务器应该开始搜索的LDAP层级的特定辨别名称，当远程用户登录和系统尝试获得用户的DN根据他们的用户名。最大支持的字符串长度是127个字符。

问题修复在2.1.1和在版本上

CSCuf19514
LDAP守护程序失败了

LDAP客户端可能失败，当初始化ssl库，如果ldap_start_tls_s呼叫采取超过时完成初始化的60秒。这能发生只装箱无效DNS条目/延迟在DNS解析。

采取步骤寻址DNS解析延迟和错误。