可维护性中的Unity Connection中的故障排除错误消息

目录

简介

本文档介绍如何对可维护性页面上常见的Cisco Unity Connection错误消息进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科 Unity Connection (CUC)
- 统一服务器的证书管理

使用的组件

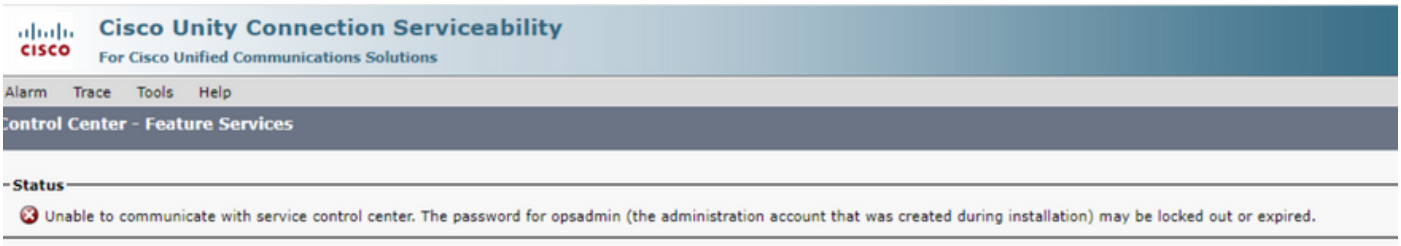
本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在Cisco Unity Connection中，当安装新节点时，必须分配用户和密码，此用户将创建并存储在Cisco Unity数据库中。

出现此错误的原因各异，导致无法使用“可维护性”页面。



要排除故障的阶段

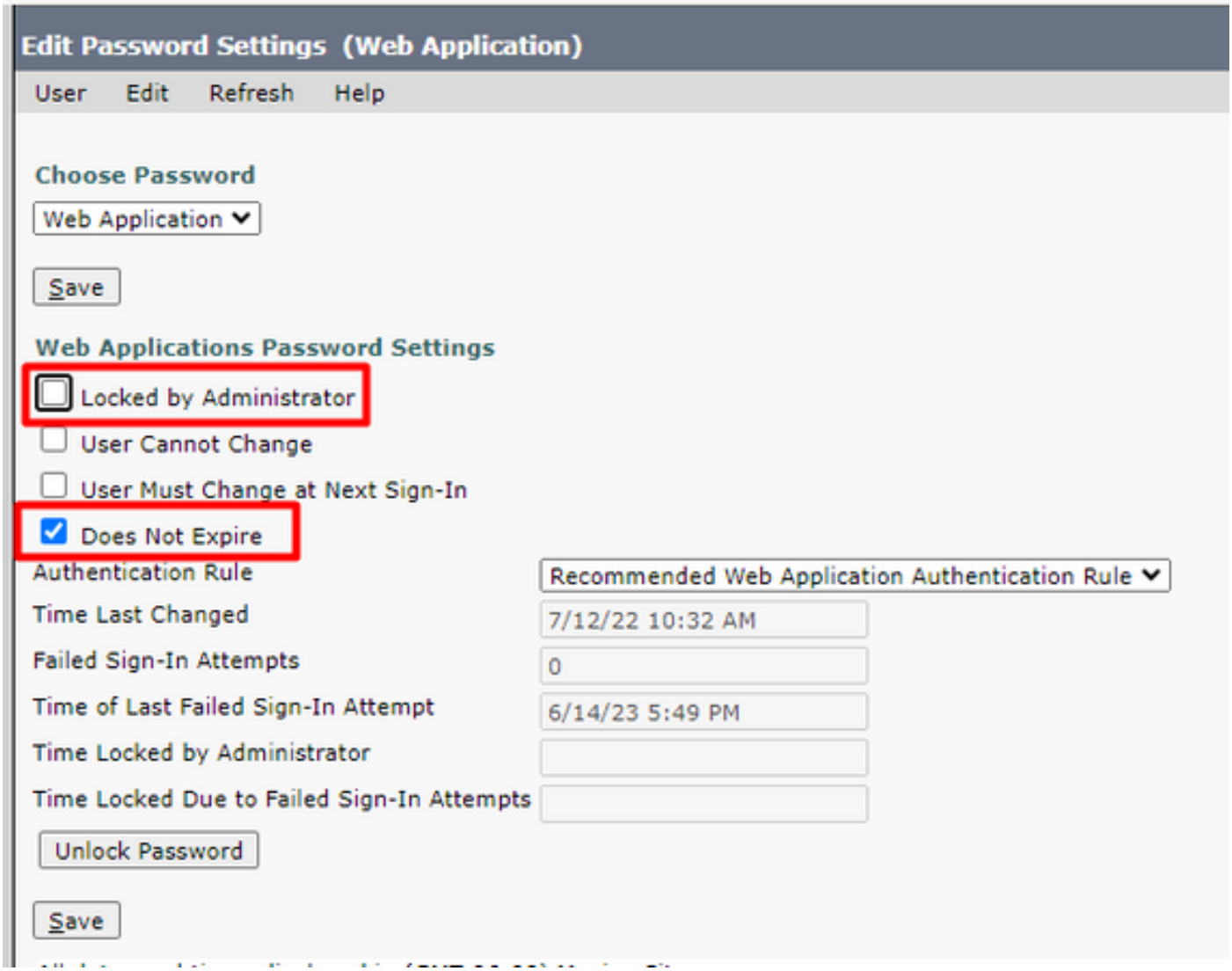
要开始排除故障，首先需要转到安装Unity时创建的管理员用户：

过程 1

导航到Cisco Unity Connection Administration > Go > Users > Select administration user > Edit > Password Settings

取消选中Locked by Administrator复选框以解锁用户帐户。

选中Does Not Expire复选框以避免密码过期。



单击Unlock Password > Save。

导航到Cisco Unity Connection可维护性页面。

过程 2

如果问题仍可复制：

导航到Cisco Unity Connection Administration > Go > Users > Select the administrator user > Edit > Change Password并输入新密码。

导航至Cisco Unity Connection Serviceability页面，验证其是否可访问。

过程 3

如果问题仍然存在：

导航到Cisco Unified OS Administration > Go > Security > Certificate Management，并验证Ipsec和Tomcat证书是否未过期。

如果证书已过期，必须重新生成证书。

再生过程：

- 自签名：自签名证书重新生成过程
- CA -signed:CA签名证书重新生成过程

过程 4

如果证书是CA签名的，您需要验证Cisco Unity Connection是否与Cisco Bug ID CSCvp31528不匹配。

如果Unity匹配，请执行以下解决方法：

解决方法1

要求CA在不使用X509v3 Subject Alternative Name（X509v3主题备用名称）的关键扩展名的情况下签署服务器证书，并让其他扩展名保持原样。

解决方法2

要求CA对服务器证书签名，并添加旁边指定的扩展使其正常工作。
X509v3基本限制：严重

解决方法3

使用自签名证书，它并不总是适合所有用户的解决方案。

解决方法4

作为最后的解决方法之一，升级到包含缺陷修复的版本，并在固定版本上生成CSR，并由CA签署（这是通过正常流程所了解的）。

过程 5

在CUC CLI上：

1.从Unity Connection数据库中检索默认应用程序管理员用户的objectID。

```
run cuc dbquery unitydirdb select name, value from vw_configuration where name='DefaultAdministrator'
```

命令输出:

```
name                  value
--------------------  -------------------------------------
DefaultAdministrator  XXXX-XXXX-XXXXX-XXXX
```

2.检索与默认应用程序管理员objectID关联的别名。查询时将字段objectid='XXXX-XXXX-XXXXX-XXXX'替换为先前输出中的值。

```
run cuc dbquery unitydirdb select alias,objectid from vw_user where objectid='XXXX-XXXX-XXXXX-XXXX'
```

命令输出:

```
alias    objectid
-----  ------------------------------------
admin  XXXX-XXXX-XXXXX-XXXX
```

3.确认加密类型为4，用于默认应用程序管理员用户的Web身份验证（Credentialtype 3用于Web应用程序密码）。

```
run cuc dbquery unitydirdb select objectid, userobjectid, credentialtype, encryptiontype from tbl_crede
```

命令输出:

```
objectid                              userobjectid                          credentialtype encryptionty
------------------------------------  ------------------------------------- -------------- ------------
ZZZZZ-ZZZZZ-ZZZZZ-ZZZZZ                 XXXX-XXXX-XXXXX-XXXX                          3              4
TTTTT-TTTTT-TTTTT-TTTTT                 XXXX-XXXX-XXXXX-XXXX                          4              3
```

如果加密类型= 3，则更改为4。

```
run cuc dbquery unitydirdb update tbl_credential set encryptiontype = "4" where objectid = "ZZZZZ-ZZZZZ
```

5.必须更改密码，因为旧密码已使用类型3对用户进行了加密

```
utils cuc reset password <accountalias>
```

6.通过CLI重新启动Tomcat

```
utils service restart Cisco Tomcat
```

验证是否可访问可维护性页面。

如果问题仍然存在，请从RTMT收集CUC Tomcat日志。

为此，请执行以下操作：

1. 打开RTMT。
2. 插入Cisco Unity Connection IP/主机名。
3. 插入用户和密码。
4. 双击Collect Files。“收集文件”窗口打开，可选择UCM服务/应用。
5. 在“选择 UCM 服务/应用”中，点击以下各项的“所有服务器”列中的复选框：

- Cisco Tomcat

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。