

# 在SMC日誌中解決"；無法找到"；的金鑰

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[問題](#)

[解決方案](#)

## 簡介

本文說明如何解決中的「無法找到密碼」錯誤 Secure Network Analytics Manager Central Management.

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Secure Network Analytics Manager 版本7.1.1或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 背景資訊

此問題在內部服務中出現 Central Management 需要憑證，例如 SNMP v3.

沒有錯誤顯示在上 Central Management 頁面本身。

此部署具有主管理器和輔助管理器。

其 `/lancope/var/logs/containers/svc-central-management.log` 主Manager上的檔案包含行條目，其中包含 "unable to find secret for" 條目。

## 問題

在主Manager中看到此錯誤 `/lancope/var/logs/containers/svc-central-management.log` 檔案，當配置更改輔助管理器配置時。任何可配置為使用身份驗證的中央管理配置部分都可能發生這種情況。

```
Apr 27 19:47:35 smc-primary docker/svc-central-management[3214]: 2020-04-27 19:47:35.369 INFO
[qtp1907431275-88280] FailoverConfigurationSender:129 - Synchronization of Primary's APPLIANCE
a39117ce-ac2b-46eb-837c-facae0cc4abc snapshot to other SMC is successful
Apr 27 19:47:36 smc-primary docker/svc-central-management[3214]: 2020-04-27 19:47:36.982 ERROR
[qtp1907431275-88310] GlobalExceptionHandler:133 - \QError processing GET
/cm/config/appliance/a39117ce-ac2b-46eb-837c-facae0cc4abc/config/internal\E
Apr 27 19:47:36 smc-primary docker/svc-central-management[3214]:
com.lancope.cm.configuration.service.SecureDataProcessingException: Unable to find secret for
'0xe9bda01ea881b262ced8e153a3d9cf2a' <-- The error
```

次Manager在同一時間拋出錯誤 /lancope/var/logs/containers/svc-cm-agent.log 檔案：

```
Apr 27 19:47:36 smc-secondary docker/svc-cm-agent[385336]: 2020-04-27 19:47:36.305 INFO
[qtp634540230-71] StandardCommandRunner:67 - Running Command(Command(commandType=APPLY_CONFIG,
commandId=9ba839e2-6770-4f21-9f7d-cbfe6782c2dc, arguments=Optional[[internetProxy,
auditLogDestination, passwordPolicy, smtp, aide, ldapSetup, dnsCache, dns, ssh, fips, ntp,
dodin, tlsApplianceIdentity, snmpAgent, tlsClientIdentities, sso, externalServices,
localResolution, networkInterfaces, openingMessage, configBackup, host, trustStore,
sessionTimeout]]))...
Apr 27 19:47:36 smc-secondary docker/svc-cm-agent[385336]: 2020-04-27 19:47:36.306 INFO
[qtp634540230-71] CommandDispatcher:30 - Running APPLY_CONFIG 9ba839e2-6770-4f21-9f7d-
cbfe6782c2dc
Apr 27 19:47:37 smc-secondary docker/svc-cm-agent[385336]: 2020-04-27 19:47:37.135 INFO
[qtp634540230-71] StandardCommandRunner:69 - Command(Command(commandType=APPLY_CONFIG,
commandId=9ba839e2-6770-4f21-9f7d-cbfe6782c2dc, arguments=Optional[[internetProxy,
auditLogDestination, passwordPolicy, smtp, aide, ldapSetup, dnsCache, dns, ssh, fips, ntp,
dodin, tlsApplianceIdentity, snmpAgent, tlsClientIdentities, sso, externalServices,
localResolution, networkInterfaces, openingMessage, configBackup, host, trustStore,
sessionTimeout]])) completed, success = false
Apr 27 19:47:37 smc-secondary docker/svc-cm-agent[385336]: 2020-04-27 19:47:37.136 INFO
[qtp634540230-71] CommandResultStoreDAO:40 -
{"replyLink": "https://10.209.6.43/cm/config/appliance/a39117ce-ac2b-46eb-837c-facae0cc4abc/command/9ba839e2-6770-4f21-9f7d-cbfe6782c2dc/apply", "commandResult": {"type": "applyConfig", "successful": false, "details": "exit
code: 1\nElementIDs without results: aide, auditLogDestination, configBackup, dns, dnsCache,
dodin, externalServices, fips, host, internetProxy, ldapSetup, localResolution,
networkInterfaces, ntp, openingMessage, passwordPolicy, sessionTimeout, smtp, snmpAgent, ssh,
sso, tlsApplianceIdentity, tlsClientIdentities, trustStore\n---STDERR---\nERROR! Attempted to
execute \"./ansible-inventory.py\" as inventory script: Inventory script (./ansible-
inventory.py) had an execution error: /usr/local/lib/python2.7/dist-
packages/urllib3/connectionpool.py:1004: InsecureRequestWarning: Unverified HTTPS request is
being made. Adding certificate verification is strongly advised. See:
https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-warnings\n
InsecureRequestWarning,\n/usr/local/lib/python2.7/dist-packages/urllib3/connectionpool.py:1004:
InsecureRequestWarning: Unverified HTTPS request is being made. Adding certificate verification
is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#ssl-
warnings\n InsecureRequestWarning,\nTraceback (most recent call last):\n File
\"/opt/service/ansible/ansible-inventory.py\", line 48, in <module>\n \"config\":
fetch_configuration(),\n File \"/opt/service/ansible/ansible-inventory.py\", line 36, in
fetch_configuration\n return r.json()['configurableElements']\n File
\"/usr/local/lib/python2.7/dist-packages/requests/models.py\", line 889, in json\n
self.content.decode(encoding), **kwargs\n File \"/usr/lib/python2.7/json/__init__.py\", line
339, in loads\n return _default_decoder.decode(s)\n File \"/usr/lib/python2.7/json/decoder.py\",
line 364, in decode\n obj, end = self.raw_decode(s, idx=_w(s, 0).end())\n File
\"/usr/lib/python2.7/json/
Apr 27 19:47:37 smc-secondary docker/svc-cm-agent[385336]: decoder.py\", line 380, in
raw_decode\n obj, end = self.scan_once(s, idx)\nValueError: Expecting \",' delimiter: line 1
column 10305 (char 10304)\n\n\n\", \"elementResults\": [\"java.util.HashMap\", {}]}}
Apr 27 19:47:37 smc-secondary docker/svc-cm-agent[385336]: 2020-04-27 19:47:37.767 INFO
[qtp634540230-71] CommandResultStoreDAO:46 - Previous command result exists. Removing it now.
```

在主Manager上，檢查 /lancope/var/services/cm/configuration/{idofsecondarysmcdirectory}/config.json 檔案。使用 jq。

/lancope/var/services/cm/configuration/idofsecondarysmcdirectory/config.json 指令。

```
primary-smc#: jq .configurableElements.snmpAgent
/lancope/var/services/cm/configuration/{idofsecondarysmcdirectory}/config.json
{
  "agentEnabled": true,
  "agentCommunity": "fakePW123",
  "agentPort": 161,
  "sysLocation": "Somecity ST",
  "sysContact": "Example User",
  "sysName": "smc-secondary.example.com",
  "sysServices": 72,
  "sysDescr": "Stealthwatch",
  "sysObjectId": "1.3.6.1.4.1.8712.1.1",
  "username": "readonly",
  "mode": "V3",
  "encryptionPass": "0xe9bda01ea881b262ced8e153a3d9cf2a", <-- This is the same value seen in the
log file from the Primary Manager
  "authPass": "0x6bb67c14beca3b6ba319485441cd24a36f80068d",
}
```

## 解決方案

導航至 **Central Management > Actions > Edit Appliance Configuration > Network Services** 然後輸入 Encryption Password 和 Authentication Password 選擇SNMP版本V3時，「SNMP代理」部分中的值。完成後，選擇 **Apply Settings**.

# Appliance Configuration - Manager

( ) / Last Updated: 11/03/2022 8:39 AM by admin

Appliance

**Network Services**

General

## SNMP Agent

Modified

Enable

Read Only Community \*

fakePW123

SNMP Port (Default 161) \*

161

SysLocation \*

Somecity ST

SysContact \*

Example User

SysName \*

smc-secondary.example.com

SysServices \*

72

SysDescription \*

Stealthwatch

SysObjectId \*

1.3.6.1.4.1.8712.1.1

SNMP Version

V2  V3

User Name \*

readonly

Encryption Password \*

.....

Authentication Password \*

.....

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。