

Resolve "Unable to Find Secret for" Error in SMC Logs

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Problem](#)

[Solution](#)

Introduction

This document describes how to resolve the "unable to find secret for" error in Secure Network Analytics Manager Central Management.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Secure Network Analytics Manager version 7.1.1 or newer

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This problem is seen in services within **Central Management** that require credentials such as **SNMP v3**.

There are no errors displayed on a Central Management page itself.

This deployment had a Primary and Secondary Manager.

The `/lancope/var/logs/containers/svc-central-management.log` file on the Primary Manager has line entries that contain "unable to find secret for" entries.

Problem

The error is seen in the Primary Manager `/lancope/var/logs/containers/svc-central-management.log` file when a configuration change is made to the Secondary Managers configuration. This can happen with any Central Management configuration section that can be configured to use authentication.

```
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
```

The Secondary Manager throws an error at the same time in the same `/lancope/var/logs/containers/svc-cm-agent.log` file:

```
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\nInsecureRequestWarning, \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\nInsecureRequestWarning, \nTraceback (most recent call last):\nFile \"/opt/service/ansible/ansible-inventory.py\", line 48, in <module>\n  \"config\":\n  fetch_configuration(),\n  File \"/opt/service/ansible/ansible-inventory.py\", line 36, in\n  fetch_configuration\n  return r.json()['configurableElements']\n  File\n  \"/usr/local/lib/python2.7/dist-packages/requests/models.py\", line 889, in\n  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  
\n/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.
```

On the Primary Manager, check the contents of
the `/lancope/var/services/cm/configuration/{idofsecondarismcdirectory}/config.json` file. with the `jq` .
`/lancope/var/services/cm/configuration/idofsecondarismcdirectory/config.json` command.

```
primary-smc#: jq .configurableElements.snmpAgent  
/lancope/var/services/cm/configuration/{idofsecondarismcdirectory}/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",  
}
```

Solution

Navigate to **Central Management > Actions > Edit Appliance Configuration > Network Services** and then enter the Encryption Password and Authentication Password values in the SNMP Agent section when SNMP VERSION V3 is selected. Once complete, select **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 *

.....