

在200/300系列託管交換機上配置安全敏感資料(SSD)屬性

目標

安全敏感資料(SSD)可保護密碼等敏感資訊，允許或拒絕使用者訪問敏感資料，並防止惡意使用者損壞配置檔案。SSD利用密碼保護資料。密碼短語類似於儲存在交換機中並用作加密金鑰的密碼。不知道密碼短語的裝置將無法對使用密碼短語的資料進行解密。

本文檔旨在說明SSD屬性頁中提供的功能。

適用裝置

- SF/SG 200和SF/SG 300系列託管交換器

軟體版本

- 1.3.0.62

SSD屬性的配置

步驟 1. 登入到Web配置實用程式，然後選擇Security > Secure Sensitive Data Management > Properties。Properties頁面隨即開啟：

Properties

Persistent Settings

Current Local Passphrase Type: Default

Configuration File Passphrase Control: Unrestricted
 Restricted

Configuration File Integrity Control: Enable

Current Session Settings

Read Mode: Plaintext
 Encrypted

Apply

Cancel

Change Local Passphrase

注意：Current Local Passphrase Control說明裝置是使用預設密碼還是使用使用者定義的密碼。

步驟 2.在「Configuration File Passphrase Control」欄位中單擊所需的單選按鈕。

·非限制 — 將密碼傳送到組態檔中，以便其他裝置知道該密碼短語。

·受限 — 限制向配置檔案傳送密碼短語，從而阻止其他裝置學習該密碼短語。

步驟 3.選中Configuration File Integrity Control覈取方塊以啟用保護，防止對配置檔案進行不需要的修改。

步驟 4.按一下Read Mode欄位中所需的單選按鈕以設定檔案的讀取方式。

·純文字檔案 — 使用純文字檔案顯示當前會話資訊。

·已加密 — 在檔案顯示會話資訊之前對其進行加密。

步驟 5.按一下Apply以保留當前更改，或按一下Cancel以撤消在頁面中進行的更改。

更改本地密碼

步驟 1.登入到Web配置實用程式，然後選擇Security > Secure Sensitive Data Management > Properties。按一下「Change Local Passphrase」。Change Local Passphrase頁面隨即開啟：

Change Local Passphrase

The minimum requirements for Local Passphrase are as follows:

- Should be at least 8 characters up to 16 characters.
- Should be at least one upper case character, one lower case character, one numeric number, and one special character e.g. #,\$.

Current Local Passphrase Type: Default

Local Passphrase: Default User Defined (Plaintext) (14/16 Characters Used)

Confirm Passphrase

Apply Cancel Back

注意：當前本地密碼型別描述了正在使用的密碼。

步驟 2.從Local Passphrase（本地密碼短語）欄位中單擊所需的單選按鈕。

·預設 — 使用預設密碼。

·使用者定義 — 使用者定義使用什麼密碼短語。

步驟 3.如果按一下了「使用者定義」，請在欄位中輸入所需的密碼，然後在「確認密碼」欄位中輸入相同的密碼短語。

步驟 4.選擇Apply以保留所做的更改，或選擇Cancel以撤消此頁上的所有更改。

步驟 5.選擇Back以返回Properties頁。

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）。