規劃FPolicy外部引擎組態

ONTAP 9

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/nas-audit/plan-fpolicy-external-engine-config-concept.html on April 20, 2024. Always check docs.netapp.com for the latest.

目錄

規劃FPolicy外部引擎組態 1
規劃FPolicy外部引擎組態 1
設定FPolicy外部引擎使用SSL驗證連線的其他相關資訊 6
憑證無法在SVM災難恢復關係中複寫非ID保留組態 7
叢集範圍內的FPolicy外部引擎、搭配MetroCluster 使用功能性和SVM災難恢復組態的限制 7
完成FPolicy外部引擎組態工作表 7

規劃FPolicy外部引擎組態

規劃FPolicy外部引擎組態

在設定FPolicy外部引擎（外部引擎）之前、您必須先瞭解建立外部引擎的意義、以及可用的組態參數。此資訊可協助您判斷要為每個參數設定哪些值。

建立FPolicy外部引擎時所定義的資訊

外部引擎組態定義FPolicy建立及管理外部FPolicy伺服器（FPolicy伺服器）連線所需的資訊、包括下列資訊：

- SVM名稱
- 引擎名稱
- 主要和次要FPolicy伺服器的IP位址、以及連接至FPolicy伺服器時要使用的TCP連接埠號碼
- 引擎類型為非同步或同步
- 如何驗證節點與FPolicy伺服器之間的連線

  如果您選擇設定相互SSL驗證、則也必須設定提供SSL憑證資訊的參數。

- 如何使用各種進階權限設定來管理連線

  這包括定義逾時值、重試值、保持活動值、最大要求值、傳送和接收緩衝區大小值、以及工作階段逾時值等項目的參數。

。`vserver fpolicy policy external-engine create` 命令用於建立 FPolicy 外部引擎。

基本的外部引擎參數是什麼

您可以使用下表的基本FPolicy組態參數來協助規劃組態：

資訊類型	選項
SVM 指定您要與此外部引擎建立關聯的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`

引擎名稱_ 指定要指派給外部引擎組態的名稱。之後建立FPolicy原則時、您必須指定外部引擎名稱。這會將外部引擎與原則建立關聯。 名稱最長可達256個字元。 ⓘ 如果在MetroCluster 一個還原或SVM災難恢復組態中設定外部引擎名稱、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • “_” 、 “-”, and “.”	`-engine-name engine_name`
主要*FPolicy*伺服器 指定節點傳送特定FPolicy原則通知的主要FPolicy伺服器。此值會指定為以逗號分隔的IP位址清單。 如果指定多個主要伺服器IP位址、則SVM參與的每個節點都會在原則啟用時、建立每個指定主要FPolicy伺服器的控制連線。如果您設定多個主要FPolicy伺服器、通知會以循環配置資源的方式傳送至FPolicy伺服器。 如果外部引擎用於MetroCluster SVM災難恢復組態、您應該將來源站台FPolicy伺服器的IP位址指定為主要伺服器。目的地站台FPolicy伺服器的IP位址應指定為次要伺服器。	`-primary-servers IP_address、 ...`
連接埠號碼_ 指定FPolicy服務的連接埠號碼。	`-port integer`
次要FPolicy伺服器_ 指定次要FPolicy伺服器、以便針對指定的FPolicy原則傳送檔案存取事件。此值會指定為以逗號分隔的IP位址清單。 次要伺服器只會在無法連線到任何一部主要伺服器時使用。當原則啟用時、就會建立次要伺服器的連線、但只有在所有主要伺服器都無法連線時、才會將通知傳送到次要伺服器。如果您設定多個次要伺服器、通知會以循環配置資源的方式傳送至FPolicy伺服器。	`-secondary-servers IP_address、 ...`

外部引擎類型_ 指定外部引擎是以同步或非同步模式運作。根據預設、FPolicy會以同步模式運作。 設定為時 `synchronous`、檔案要求處理會傳送通知給 FPolicy 伺服器、但在收到 FPolicy 伺服器的回應之後才會繼續。此時、視FPolicy伺服器的回應是否允許要求的動作而定、要求流程會繼續或處理會導致拒絕。 設定為時 `asynchronous`、檔案要求處理會傳送通知給 FPolicy 伺服器、然後繼續。	`-extern-engine-type external_engine_type` 此參數的值可以是下列其中一項： • `synchronous` • `asynchronous`
與FPolicy server_通訊的_SSL選項 指定與FPolicy伺服器通訊的SSL選項。這是必要的參數。您可以根據下列資訊選擇其中一個選項： • 設定為時 `no-auth`、不進行驗證。 通訊連結是透過TCP建立。 • 設定為時 `server-auth`， SVM 使用 SSL 伺服器驗證來驗證 FPolicy 伺服器。 • 設定為時 `mutual-auth`、在 SVM 和 FPolicy 伺服器之間進行相互驗證； SVM 驗證 FPolicy 伺服器、 FPolicy 伺服器驗證 SVM 。 如果您選擇設定相互 SSL 驗證、則也必須設定 `-certificate -common-name`、 `-certificate-serial`和 `-certifcate-ca` 參數。	`-ssl-option {no-auth`
`server-auth`	`mutual-auth}`
憑證*FQDN*或自訂通用名稱 指定在SVM與FPolicy伺服器之間設定SSL驗證時所使用的憑證名稱。您可以將憑證名稱指定為FQDN或自訂通用名稱。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-common-name` 參數。	`-certificate-common -name text`
憑證序號 指定在SVM與FPolicy伺服器之間設定SSL驗證時、用於驗證的憑證序號。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-serial` 參數。	`-certificate-serial text`

憑證授權單位 指定在SVM與FPolicy伺服器之間設定SSL驗證時、用於驗證的憑證CA名稱。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-ca` 參數。	`-certificate-ca text`

進階的外部引擎選項是什麼

您可以在規劃是否使用進階參數自訂組態時、使用下表的進階FPolicy組態參數。您可以使用這些參數來修改叢集節點與FPolicy伺服器之間的通訊行為：

資訊類型	選項
取消要求的逾時_ 指定時間間隔（小時）（`h`）、分鐘 (`m`）或秒 (`s`）節點等待 FPolicy 伺服器的回應。 如果逾時時間間隔超過、節點會將取消要求傳送至FPolicy伺服器。然後、節點會將通知傳送至替代的FPolicy伺服器。此逾時有助於處理無回應的FPolicy伺服器、進而改善SMB/NFS用戶端回應。此外、在逾時期間之後取消要求、也有助於釋出系統資源、因為通知要求會從停機/不良的FPolicy伺服器移至替代的FPolicy伺服器。 此值的範圍為 `0` 透過 `100`。如果值設為 `0`，此選項已停用，取消要求訊息不會傳送至 FPolicy 伺服器。預設值為 `20s`。	`-reqs-cancel-timeout integer`[h
m	s]
中止要求的逾時_ 指定逾時（以小時為單位）（`h`）、分鐘 (`m`）或秒 (`s`）以中止要求。 此值的範圍為 `0` 透過 `200`。	`-reqs-abort-timeout` ` `integer`[h
m	s]
傳送狀態要求的時間間隔 指定以小時為單位的時間間隔 (`h`）、分鐘 (`m`）或秒 (`s`）之後、狀態要求會傳送至 FPolicy 伺服器。 此值的範圍為 `0` 透過 `50`。如果值設為 `0`、選項已停用、狀態要求訊息不會傳送至 FPolicy 伺服器。預設值為 `10s`。	`-status-req-interval integer`[h
m	s]

*FPolicy*伺服器上未處理的要求上限 指定可在FPolicy伺服器上排入佇列的未處理要求數目上限。 此值的範圍為 1 透過 10000。預設值為 500。	-max-server-reqs integer
中斷無回應的*FPolicy*伺服器連線逾時 指定時間間隔（小時）（h）、分鐘 (m）或秒 (s）之後、會終止與 FPolicy 伺服器的連線。 只有FPolicy伺服器的佇列包含允許的最大要求數、且在逾時期間內未收到任何回應時、才會在逾時期間之後終止連線。允許的最大要求數為其中之一 50（預設）或指定的號碼 max-server-reqs- 參數。 此值的範圍為 1 透過 100。預設值為 60s。	-server-progress -timeout integer[h
m	s]
_將保持活動訊息傳送至FPolicy server_的時間間隔 指定時間間隔（小時）（h）、分鐘 (m）或秒 (s）將保持活動的訊息傳送到 FPolicy 伺服器。 「保持連線」訊息會偵測半開啟的連線。 此值的範圍為 10 透過 600。如果值設為 0，此選項會停用，並防止將持續作用的訊息傳送至 FPolicy 伺服器。預設值為 120s。	-keep-alive-interval- integer[h
m	s]
最大重新連線嘗試次數_ 指定SVM在連線中斷後嘗試重新連線至FPolicy伺服器的最大次數。 此值的範圍為 0 透過 20。預設值為 5。	-max-connection-retries integer
接收緩衝區大小_ 指定FPolicy伺服器之連接插槽的接收緩衝區大小。 預設值設為256 KB。當值設定為0時、接收緩衝區的大小會設定為系統定義的值。 例如、如果套接字的預設接收緩衝區大小為65536位元組、將可調值設為0、則套接字緩衝區大小會設為65536位元組。您可以使用任何非預設值來設定接收緩衝區的大小（以位元組為單位）。	-recv-buffer-size integer

傳送緩衝區大小 指定FPolicy伺服器之連線通訊端的傳送緩衝區大小。 預設值設為256 KB。當值設定為0時、傳送緩衝區的大小會設定為系統定義的值。 例如、如果套接字的預設傳送緩衝區大小設為65536位元組、將可調值設為0、則套接字緩衝區大小會設為65536位元組。您可以使用任何非預設值來設定傳送緩衝區的大小（以位元組為單位）。	`-send-buffer-size integer`
重新連線期間清除工作階段*ID*逾時 指定以小時為單位的時間間隔 (`h`）、分鐘 (`m`）或秒 (`s`）之後、新的工作階段 ID 會在重新連線嘗試期間傳送至 FPolicy 伺服器。 如果儲存控制器與FPolicy伺服器之間的連線終止、並在中進行重新連線 `-session-timeout` 時間間隔時、舊的工作階段ID會傳送至FPolicy伺服器、以便傳送舊通知的回應。 預設值設為 10 秒。	`-session-timeout [integerh][integerM][integers]`

設定FPolicy外部引擎使用SSL驗證連線的其他相關資訊

如果您想要設定FPolicy外部引擎、以便在連線至FPolicy伺服器時使用SSL、您需要知道一些其他資訊。

SSL伺服器驗證

如果您選擇將FPolicy外部引擎設定為SSL伺服器驗證、則在建立外部引擎之前、必須先安裝簽署FPolicy伺服器憑證的憑證授權單位（CA）的公開憑證。

相互驗證

如果您將FPolicy外部引擎設定為在將儲存虛擬機器（SVM）資料LIF連線至外部FPolicy伺服器時使用SSL相互驗證、則在建立外部引擎之前、 您必須安裝簽署FPolicy伺服器憑證的CA公開憑證、以及用於驗證SVM的公開憑證和金鑰檔。當任何FPolicy原則使用已安裝的憑證時、您不得刪除此憑證。

如果在FPolicy連線至外部FPolicy伺服器時、憑證被刪除、則無法重新啟用使用該憑證的停用FPolicy原則。在這種情況下、即使在SVM上建立並安裝了具有相同設定的新憑證、也無法重新啟用FPolicy原則。

如果憑證已刪除、您需要安裝新的憑證、建立使用新憑證的新FPolicy外部引擎、並透過修改FPolicy原則、將新的外部引擎與您要重新啟用的FPolicy原則建立關聯。

安裝SSL憑證

用來簽署 FPolicy 伺服器憑證的 CA 公用憑證是使用安裝 `security certificate install` 命令 `-type` 參數設為 `client-ca`。使用安裝驗證 SVM 所需的私密金鑰和公開憑證 `security certificate install` 命令 `-type` 參數設為 `server`。

憑證無法在SVM災難恢復關係中複寫非ID保留組態

連線至FPolicy伺服器時用於SSL驗證的安全性憑證、不會以非ID-preserve組態複寫至SVM災難恢復目的地。雖然已複寫SVM上的FPolicy外部引擎組態、但不會複寫安全性憑證。您必須在目的地上手動安裝安全性憑證。

當您設定 SVM 災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、所有 FPolicy 組態詳細資料都會複寫、包括安全性憑證資訊。只有當您將選項設定為時、才必須在目的地上安裝安全性憑證 `false` （非 ID-Preserve ）。

叢集範圍內的FPolicy外部引擎、搭配MetroCluster 使用功能性和SVM災難恢復組態的限制

您可以將叢集儲存虛擬機器（SVM）指派給外部引擎、藉此建立叢集範圍內的FPolicy外部引擎。然而、在MetroCluster 使用叢集或SVM災難恢復組態建立以叢集為範圍的外部引擎時、選擇SVM用於與FPolicy伺服器進行外部通訊的驗證方法時、會有某些限制。

建立外部FPolicy伺服器時、您可以選擇三種驗證選項：無驗證、SSL伺服器驗證和SSL相互驗證。雖然在選擇驗證選項時沒有任何限制、但如果將外部FPolicy伺服器指派給資料SVM、則在建立叢集範圍的FPolicy外部引擎時仍有限制：

組態	是否允許？
不含驗證的SVM災難恢復和叢集範圍的FPolicy外部引擎（未設定SSL）MetroCluster	是的
包含SSL伺服器或SSL相互驗證的SVM災難恢復、以及叢集範圍的FPolicy外部引擎MetroCluster	否

- 如果存在具有SSL驗證的叢集範圍FPolicy外部引擎、而您想要建立MetroCluster 一套支援還原或SVM災難恢復的組態、您必須先修改此外部引擎、使其不使用驗證、或是移除外部引擎、才能建立MetroCluster 還原或SVM災難恢復組態。
- 如果MetroCluster 已存在支援功能的不支援功能或SVM災難恢復組態、ONTAP 則無法使用SSL驗證來建立叢集範圍的FPolicy外部引擎。

完成FPolicy外部引擎組態工作表

您可以使用這份工作表來記錄FPolicy外部引擎組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的使用值、再設定外部引擎。

基本外部引擎組態資訊

您應該記錄是否要在外部引擎組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
引擎名稱	是的	是的	
主要FPolicy伺服器	是的	是的	
連接埠號碼	是的	是的	
次要FPolicy伺服器	否		
外部引擎類型	否		
用於與外部FPolicy伺服器通訊的SSL選項	是的	是的	
憑證FQDN或自訂通用名稱	否		
憑證序號	否		
憑證授權單位	否		

進階外部引擎參數資訊

若要使用進階參數設定外部引擎、您必須在進階權限模式下輸入組態命令。

資訊類型	必要	包括	您的價值
取消要求逾時	否		
中止要求的逾時	否		
傳送狀態要求的時間間隔	否		
FPolicy伺服器上未處理的要求上限	否		
中斷無回應的FPolicy伺服器連線逾時	否		
將「保持作用中」訊息傳送至FPolicy伺服器的時間間隔	否		
最大重新連線嘗試次數	否		

接收緩衝區大小	否		
傳送緩衝區大小	否		
重新連線期間清除工作階段ID的逾時	否		

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。