Planen Sie die FPolicy-Konfiguration

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

Planen Sie die FPolicy-Konfiguration

Planen Sie die FPolicy-Konfiguration im Überblick

Bevor Sie die FPolicy konfigurieren, müssen Sie verstehen, welche Parameter beim Erstellen der Richtlinie erforderlich sind sowie warum Sie bestimmte optionale Parameter konfigurieren möchten. Anhand dieser Informationen können Sie festlegen, welche Werte für jeden Parameter festgelegt werden sollen.

Beim Erstellen einer FPolicy verknüpfen Sie die Richtlinie mit der folgenden:

- Die Storage Virtual Machine (SVM)
- Ein oder mehrere FPolicy Events
- Eine externe FPolicy Engine

Sie können auch mehrere optionale Richtlinieneinstellungen konfigurieren.

Was die FPolicy-Konfiguration enthält

Sie können die folgende Liste der erforderlichen FPolicy und optionalen Parameter verwenden, um Ihre Konfiguration zu planen:

Informationstyp	Option	Erforderlich	Standard
SVM Name Gibt den Namen der SVM an, auf der eine FPolicy erstellt werden soll.	`-vserver vserver_name`	Ja.	Keine

Name der Richtlinie Gibt den Namen der FPolicy an. Der Name kann bis zu 256 Zeichen lang sein. Wenn die Richtlinie in einer MetroCluster- oder SVM-Disaster-Recovery-Konfiguration konfiguriert ist, sollte der Name bis zu 200 Zeichen lang sein. Der Name kann eine beliebige Kombination der folgenden Zeichen des ASCII-Bereichs enthalten: • `a` Bis `z` • `A` Bis `Z` • `0` Bis `9` • „_“, „-`", and ".`“	`-policy-name policy_name`	Ja.	Keine
Ereignisnamen Gibt eine kommagetrennte Liste von Ereignissen an, die mit der FPolicy verknüpft werden sollen. • Sie können einer Richtlinie mehrere Ereignisse zuordnen. • Ein Ereignis ist spezifisch für ein Protokoll. • Sie können eine einzelne Richtlinie verwenden, um Dateizugriffsereignisse für mehr als ein Protokoll zu überwachen, indem Sie für jedes Protokoll, das die Richtlinie überwachen soll, ein Ereignis erstellen und dann die Ereignisse mit der Richtlinie verknüpfen. • Die Ereignisse müssen bereits vorhanden sein.	`-events event_name, ...`	Ja.	Keine

Name der externen Engine Gibt den Namen der externen Engine an, die mit der FPolicy verknüpft werden soll. • Eine externe Engine enthält die vom Knoten benötigten Informationen zum Senden von Benachrichtigungen an einen FPolicy-Server. • Sie können FPolicy so konfigurieren, dass die native externe ONTAP Engine zum einfachen Blockieren von Dateien oder zur Verwendung einer externen Engine verwendet wird, die für die Verwendung von externen FPolicy-Servern (FPolicy-Servern) konfiguriert ist, um anspruchsvollere Datei-Blockierung und Dateimanagement zu ermöglichen. • Wenn Sie die native externe Engine verwenden möchten, können Sie entweder keinen Wert für diesen Parameter angeben oder angeben `native` Als Wert. • Wenn Sie FPolicy-Server verwenden möchten, muss die Konfiguration für die externe Engine bereits vorhanden sein.	`-engine engine_name`	Ja (es sei denn, diese Richtlinie nutzt die interne ONTAP-native Engine)	`native`
Ist obligatorisches Screening erforderlich Gibt an, ob eine obligatorische Überprüfung des Dateizugriffs erforderlich ist. • Die obligatorische Screening-Einstellung legt fest, welche Maßnahmen bei einem Dateizugriff getroffen werden sollen, wenn alle primären und sekundären Server ausgefallen sind oder keine Antwort von den FPolicy-Servern innerhalb eines bestimmten Zeitlimits erhalten wird. • Wenn eingestellt auf `true`, Dateizugriffsereignisse werden verweigert. • Wenn eingestellt auf `false`, Dateizugriffsereignisse sind erlaubt.	`-is-mandatory {true`	`false}`	Nein

`true`	*Privilegierten Zugriff zulassen* Gibt an, ob der FPolicy-Server über eine privilegierte Datenverbindung privilegierten Zugriff auf die überwachten Dateien und Ordner haben soll. Bei entsprechender Konfiguration können FPolicy Server über die privilegierte Datenverbindung auf Dateien vom Root der SVM zugreifen, die die überwachten Daten enthalten. Für den privilegierten Datenzugriff muss SMB auf dem Cluster lizenziert sein. Alle Daten-LIFs für die Verbindung mit den FPolicy Servern müssen konfiguriert werden `cifs` Als eines der zulässigen Protokolle. Wenn Sie die Richtlinie so konfigurieren möchten, dass ein privilegierter Zugriff möglich ist, müssen Sie auch den Benutzernamen für das Konto angeben, das der FPolicy-Server für privilegierten Zugriff verwenden soll.	`-allow -privileged -access` {`yes`	`no`}

Nein (es sei denn, Passthrough-read ist aktiviert)	`no`	*Privilegierter Benutzername* Gibt den Benutzernamen des Kontos an, das FPolicy-Server für privilegierten Datenzugriff verwenden. • Der Wert für diesen Parameter sollte das Format „`domain\userName`“ verwenden. • Wenn `-allow-privileged-access` Ist auf festgelegt `no`, Jeder für diesen Parameter eingestellte Wert wird ignoriert.	`-privileged-user-name user_name`

Nein (sofern der privilegierte Zugriff nicht aktiviert ist)	Keine	*Passthrough-read* zulassen Gibt an, ob die FPolicy-Server PassThrough-Read-Services für Dateien bereitstellen können, die von den FPolicy-Servern in sekundären Speicher (Offline-Dateien) archiviert wurden: • Passthrough-read ist eine Möglichkeit, Daten von Offline-Dateien zu lesen, ohne die Daten auf den primären Speicher wiederherzustellen. Durch das Passthrough-Lesevorgang werden die Reaktionszeiten reduziert, da vor der Reaktion auf die Leseanforderung keine Dateien zurück auf den primären Storage zurückgerufen werden müssen. Zusätzlich optimiert das Passthrough-Lesevorgang die Storage-Effizienz, da es nicht mehr erforderlich ist, primären Storage mit Dateien zu belegen, die ausschließlich für Lesezugriffe abgerufen werden.	`-is-passthrough-read-enabled {true`

Anforderung für FPolicy-Konfigurationen, wenn die FPolicy die native Engine verwendet

Wenn Sie die FPolicy so konfigurieren, dass die native Engine verwendet wird, gibt es eine spezifische Anforderung dafür, wie Sie den FPolicy-Umfang definieren, der für die Richtlinie konfiguriert ist.

FPolicy-Umfang definiert die Grenzen, über die die FPolicy gilt, zum Beispiel, ob FPolicy auf bestimmte Volumes oder Freigaben angewendet wird. Es gibt eine Reihe von Parametern, die den Geltungsbereich der FPolicy weiter einschränken. Einer dieser Parameter, `-is-file-extension-check-on-directories-enabled`, Gibt an, ob Dateierweiterungen auf Verzeichnissen überprüft werden sollen. Der Standardwert ist `false`, Das bedeutet, dass Dateierweiterungen auf Verzeichnissen nicht überprüft werden.

Wenn eine FPolicy, die die native Engine nutzt, auf einem Share oder Volume die `-is-file-extension-check-on-directories-enabled` Parameter ist auf festgelegt `false` Für den Umfang der Richtlinie wird der Zugriff auf das Verzeichnis verweigert. Da die Verzeichnisse überprüft werden, wird bei dieser Konfiguration ein Verzeichnisvorgang unter den Geltungsbereich der Richtlinie fällt.

Um sicherzustellen, dass der Verzeichniszugriff erfolgreich ist, wenn Sie die native Engine verwenden, müssen Sie den festlegen `-is-file-extension-check-on-directories-enabled` Parameter Bis `true` Beim Erstellen des Anwendungsbereichs.

Wenn dieser Parameter auf gesetzt ist `true`, Erweiterungsprüfungen erfolgen für Verzeichnisvorgänge und die Entscheidung, ob der Zugriff erlaubt oder verweigert wird, wird auf Grundlage der in der FPolicy Scope-Konfiguration enthaltenen oder ausgeschlossenen Erweiterungen getroffen.

Wenn diese Option aktiviert ist, stellen die FPolicy-Server die Daten für die Datei über einen separaten privilegierten Datenkanal bereit, der speziell für Passdurchlesevorgänge geöffnet wurde.

- Wenn Sie die Richtlinie so konfigurieren möchten, dass der privilegierte Zugriff für Verzeichnisvorgänge und die

Füllen Sie das FPolicy-Arbeitsblatt aus

Mit diesem Arbeitsblatt können Sie die Werte erfassen, die Sie während der Konfiguration der Richtlinien für FPolicy benötigen. Sie sollten aufzeichnen, ob Sie die einzelnen Parametereinstellungen in die FPolicy-Konfiguration aufnehmen möchten, und dann den Wert für die Parameter notieren, die Sie einbeziehen möchten.

Informationstyp	Einschließlich	Ihre Werte
Name der Storage Virtual Machine (SVM	Ja.	
Name der Richtlinie	Ja.	
Ereignisnamen	Ja.	
Name der externen Engine		
Ist ein obligatorisches Screening erforderlich?		
Privilegierten Zugriff zulassen		

Privilegierter Benutzername		
Ist Passthrough-read aktiviert?		