

保護工作負載 BlueXP ransomware protection

NetApp October 07, 2024

This PDF was generated from https://docs.netapp.com/zh-tw/bluexp-ransomware-protection/rp-use-protect.html on October 07, 2024. Always check docs.netapp.com for the latest.

目錄

保護工作負載	 	 	1
使用勒索軟體策略保護工作負載	 	 	1

保護工作負載

使用勒索軟體策略保護工作負載

您可以使用 BlueXP 勒索軟體保護來完成下列動作、以保護工作負載免受勒索軟體攻擊。

- 啟用工作負載一致的保護功能、可與 SnapCenter 軟體或 SnapCenter Plug-in for VMware vSphere 搭配使用。
- •建立或管理勒索軟體保護策略、包括您為快照、備份和勒索軟體保護所建立的原則(稱為 _ 偵測原則 _)。
- 匯入策略並加以調整。
- 群組檔案共用、讓您更容易保護工作負載、而非個別保護工作負載。
- 刪除勒索軟體保護策略。
- •哪些服務用於保護? *下列服務可用於管理保護原則。BlueXP 勒索軟體保護中會顯示這些服務的保護資訊
- 檔案共用、 VM 檔案共用的 BlueXP 備份與還原
- 適用於 VMware 的 SnapCenter for VM 資料存放區
- SnapCenter for Oracle 和 MySQL

保護原則

您可能會發現檢閱有關您可以變更的保護原則、以及保護策略中的原則類型等資訊很有幫助。

• 您可以變更哪些保護原則? *

您可以根據擁有的工作負載保護來變更保護原則:

- * 工作負載不受 NetApp 應用程式保護 * :這些工作負載並非由 SnapCenter、 SnapCenter Plug-in for VMware vSphere 或 BlueXP 備份與還原所管理。這些工作負載可能會將快照當成 ONTAP 或其他產品的一 部分。如果 ONTAP FPolicy 保護已就緒、您可以使用 ONTAP 變更 FPolicy 保護。
- * 由 NetApp 應用程式提供現有保護的工作負載 * :這些工作負載具有由 SnapCenter 、 SnapCenter for VMware vSphere 或 BlueXP 備份與還原所管理的備份或快照原則。
 - [。]如果快照或備份原則是由 SnapCenter 、 SnapCenter for VMware 或 BlueXP 備份與還原管理、則這些 原則將繼續由這些應用程式管理。使用 BlueXP 勒索軟體保護、您也可以將勒索軟體偵測原則套用至這 些工作負載。
 - [。]如果勒索軟體偵測原則是由 ONTAP 中的自主勒索軟體保護(ARP)和 FPolicy 管理、則這些工作負載 會受到保護、並將繼續由 ARP 和 FPolicy 管理。
- 勒索軟體保護策略需要哪些政策? *

勒索軟體保護策略需要下列原則:

- 勒索軟體偵測原則
- Snapshot原則

BlueXP 勒索軟體保護策略不需要備份原則。

檢視工作負載的勒索軟體保護

保護工作負載的第一步之一、就是檢視您目前的工作負載及其保護狀態。您可以看到下列類型的工作負載:

- 應用程式工作負載
- VM 工作負載
- 檔案共用工作負載

步驟

- 1. 從 BlueXP 左側瀏覽器中、選取 * 保護 * > * 勒索軟體保護 * 。
- 2. 執行下列其中一項:
 - 。從儀表板的資料保護窗格中、選取*檢視全部*。
 - 。從功能表中選取*保護*。

0 16 MINK 0 414975	lays()		32 Gið Duta at rísk			7 Potects 1 (Last 7	rd (D) 7 deyrs	14 Giß Data protecta	¢		
WorkSoads	·	Protection grou	н								
Workloads (24)									٩	1 Manage p	objection strategies
workload =	ηpe τ≑	Connector 0	Importance # \$	O Muscy e_ 1	Protection # :	Protection # \$	Detection T 2	Detection _ T =	Snapshot T \$	Backup desti 🗧	
Vm_datamore_uneau	VM Ne share	ave-connector-us	pricel	69	🕑 Protected	6/9	Adhe	rps-policy-ad	Budd tareonika	netapp-backup-vs	(FOR protection)
Vm_datastrine_unnery	VM file share	ave-connector-us	Critical	0.9	Protected	n'a	Learning mode	rps-policy-all	Buel? lanomisa.,	netapp-backup-vs.,	
Vm, datastore, uswer	vM file share	ave convector-us.	therdard	n/8	🗇 "At mik	0.9	None	Note	None	netapp-backup-vs	Protect
Virg datastore juwer	vM Ne share	avs connector-us	that shared	n/a	🛈 "Atrisk	n/a	None	None	None	netopp-backup-vs	Protect
Vm_datastone_useas	VM file share	ave-connector-us	Standard	0/3	() At the	0/3	None	None	Nore	netapp-backup-us	Promet
Ver, datastow, 201, J	vvi file share	onprem-connecto	Standard	na	.Atrok	na	None	hore	None	netapp-backup-vs	Protect

3. 您可以在此頁面檢視及變更工作負載的保護詳細資料。

對於已有 SnapCenter 或 BlueXP 備份與還原服務保護原則的工作負載、您無法編輯保護。對於 這些工作負載、如果 BlueXP 勒索軟體已在其他服務中啟動、則 BlueXP 勒索軟體可啟用自動勒 索軟體保護及 / 或 FPolicy 保護。深入瞭解 "自主勒索軟體保護"、 "BlueXP 備份與還原"和 "ONTAP FPolicy"。

保護詳細資料請參閱保護頁面

(i)

「保護」頁面顯示工作負載保護的下列資訊:

- 保護狀態 * :工作負載可顯示下列其中一個保護狀態、以指出是否套用原則:
- •*受保護*:套用原則。所有與工作負載相關的磁碟區都會啟用 ARP。
- * 風險 *:不套用任何原則。如果工作負載未啟用主要偵測原則、即使已啟用快照和備份原則、也會有「風險」。
- •*進行中*:正在套用原則、但尚未完成。
- •*失敗*:套用原則但無法運作。

- 偵測狀態 * : 工作負載可具有下列其中一種勒索軟體偵測狀態:
- •*學習*:最近指派了勒索軟體偵測原則給工作負載、服務正在掃描工作負載。
- * Active * :已指派勒索軟體偵測保護原則。
- •*未設定*:未指派勒索軟體偵測保護原則。
- •* 錯誤*:已指派勒索軟體偵測原則、但服務發生錯誤。



在 BlueXP 勒索軟體保護中啟用保護功能時、警示偵測和報告會在勒索軟體偵測原則狀態從「學習」模式變更為「主動」模式後開始。

- 偵測原則 * :如果已指派勒索軟體偵測原則、則會顯示該原則的名稱。如果尚未指派偵測原則、則會顯示「 N/A」。
- Snapshot 與備份原則 * :此欄顯示套用至工作負載的快照與備份原則、以及管理這些原則的產品或服務。
- 由 SnapCenter 管理
- 由 SnapCenter Plug-in for VMware vSphere 管理
- •由 BlueXP 備份與還原管理
- 管理快照和備份的勒索軟體保護原則名稱
- 無
- 工作負載重要性 *

BlueXP 勒索軟體保護會根據每個工作負載的分析、在探索期間為每個工作負載指派重要或優先順序。工作負載 重要性取決於下列快照頻率:

- •* 關鍵*:每小時拍攝超過1份快照複本(極具挑戰性的保護排程)
- •*重要*:快照複本每小時拍攝不到1份、但每天超過1份
- •*標準*:每天拍攝超過1份快照複本
- 預先定義的偵測原則 *

您可以選擇符合工作負載重要性的下列 BlueXP 勒索軟體保護預先定義原則之一:

原則層級	Snapshot	頻率	保留(天數)	快照複本數量	快照複本總數上 限
* 關鍵工作 負載原則 *	每季一次	每 15 分鐘	3.	288	309
	每日	每1天	14.	14.	309
	每週	每1週	35	5.	309
	每月	每 30 天	60	2.	309

原則層級	Snapshot	頻率	保留(天數)	快照複本數量	快照複本總數上 限
* 重要工作 負載原則 *	每季一次	每 30 分鐘一次	3.	144.	165
	每日	每1天	14.	14.	165
	每週	每1週	35	5.	165
	每月	每 30 天	60	2.	165
* 標準工作 負載原則 *	每季一次	每 30 分鐘	3.	72.	93
	每日	每1天	14.	14.	93
	每週	每1週	35	5.	93
	每月	每 30 天	60	2.	93

使用 SnapCenter 實現應用程式或 VM 一致的保護

啟用應用程式或 VM 一致的保護功能、可協助您以一致的方式保護應用程式或 VM 工作負載、達到靜止且一致的狀態、以避免日後需要恢復時可能發生的資料遺失。

此程序會針對使用 BlueXP 備份與還原的虛擬機器、起始登錄適用於應用程式的 SnapCenter 軟體伺服器或適用 於 VMware vSphere 的 SnapCenter 外掛程式。

啟用工作負載一致的保護之後、您就可以在 BlueXP 勒索軟體保護中管理保護策略。保護策略包括在其他地方管 理的快照和備份原則、以及在 BlueXP 勒索軟體保護中管理的勒索軟體偵測原則。

若要深入瞭解如何使用 BlueXP 備份與還原為 VMware vSphere 註冊 SnapCenter 或 SnapCenter 外掛程式、請 參閱下列資訊:

- "註冊 SnapCenter 伺服器軟體"
- "註冊SnapCenter VMware vSphere的VMware外掛程式"

步驟

- 1. 從 BlueXP 勒索軟體保護功能表中、選取 * 儀表板 * 。
- 2. 從「建議」窗格中、找到下列其中一項建議、然後選取*「審查與修正」*:
 - [。]在 BlueXP 中註冊可用的 SnapCenter 伺服器
 - ◎ 在 BlueXP 中註冊 VMware vSphere (SCV)可用的 SnapCenter 外掛程式
- 3. 請依照相關資訊、使用 BlueXP 備份與還原、為 VMware vSphere 主機註冊 SnapCenter 或 SnapCenter 外 掛程式。
- 4. 返回 BlueXP 勒索軟體保護。

- 5. 從 BlueXP 勒索軟體保護開始、請前往儀表板、再次啟動探索程序。
- 6. 從 BlueXP 勒索軟體保護中、選取 * 保護 * 以檢視保護頁面。

7. 檢閱「保護」頁面上「快照與備份原則」欄中的詳細資料、查看原則是否在其他地方受到管理。

新增勒索軟體保護策略

您可以為工作負載新增勒索軟體保護策略。執行方式取決於快照和備份原則是否已經存在:

- * 如果您沒有快照或備份原則、請建立勒索軟體保護策略 * 。如果工作負載上不存在快照或備份原則、您可以建立勒索軟體保護策略、其中包括您在 BlueXP 勒索軟體保護中建立的下列原則:
 - [。]Snapshot原則
 - 。備份原則
 - 。勒索軟體偵測原則
- * 為已有快照和備份原則 * 的工作負載建立偵測原則、這些原則可在其他 NetApp 產品或服務中管理。偵測 原則不會變更在其他產品中管理的原則。

建立勒索軟體保護策略(如果您沒有快照或備份原則)

如果工作負載上不存在快照或備份原則、您可以建立勒索軟體保護策略、其中包括您在 BlueXP 勒索軟體保護 中建立的下列原則:

- Snapshot原則
- 備份原則
- 勒索軟體偵測原則

建立勒索軟體保護策略的步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。

16 40471	tay4))		32 cie Data at risk				7 Protects 1 (Let 7	d D deys	14 Giß Deta protecte	¢		
WorkSoads		Protection grou										
Workloads (24)										٩	4 Manage p	obection strategies
Workload \$	type va	Connector 2	Importance T 2	O Musys. :	Protect	601. T \$	Protection # \$	Detection _ T 2	Detection _ T \$	Snapshot _ T \$	Backup desti 🗧	
We datamane unear	VM Ne share	ave-connector-us	pricel	49	۰ 🤤	Protected	e/a	Active	rps-policy-ad	Build? (anomica	netapp-backup-vs	(Fet potenter)
Vm_datactive_unvery	VM file share	ava-connector-us	Critical	0.9	9 :	Protected	n/a	Learning mode	rps-policy-all	Buell? lansomeau	netapp-backup-vs	(Les proversam)
Vm_datastime_uswer	vM file share	ives connector-up	Mandard	n/a	0	At risk	n.¥	None	None	None	netapp-backup-vs	Protect
Virg datastine jusies	vM Ne share	ans connector-us	standard	n/a	0.	at risk	e/4	None	None	None	netapp-taskup-vs	Protect
Vm_datastore_useas	VM-file share	ave-connector-us	Standard	n/a	0	Ad visik	n/a	None	None	None	rietapp-backup-vic	Promet
Wei datastow, 201, 3	VV file share	onprem-connecto	Standard	nà	0	At risk	na	None	None	None	netapp-backup-vs	Protect

2. 從「保護」頁面選取*管理保護策略*。

1	Protection 3 Ransonware protection strategies							
			Ransomware protection	on strategies				
	Ransomware protection strategies (I)				Q	±	A65	
	Rationroware problection shateey	 Snamhot policy 	2 Backup policy	Detection policy	Protected workloads	10.1		
			and an approximately a second s					
	epi-strategy-ortical	initial-si-policy	orisial-bu-policy	rpt-policy-all	3		~	
	rpi-strategy-important	important-sz-policy	important-bu-policy	rps-policy-all	10 E		\sim	()
	spu-strategy-standard	standard-surpciley	(tandard bu golicy	tps-policy-all	0		\sim	
	Rantoenvare protection strategy- rgsi-strategy-ortical rgsi-strategy-important rgsi-strategy-intenderd	 Snapshot policy shtical-si-policy implortant-si-policy stanillard-si-policy 	Backup policy oritical bu-policy important-bu-policy (tandard-bu-policy	C I Detection policy gro-policy-all gro-policy-all gro-policy-all	3 τ ο	. ÷ †	- > > >	

3. 從勒索軟體保護策略頁面、選取 * 新增 * 。

Protection > Manage protection strategies > Add ransomware p	protection strategy				
			Add ransomware p	rotection strategy	
	Ransomware protection strategy name			Copy from existing ransomware protection strategy	
	RPS strategy 1			No policy selected	🗗 Select
	Detection policy	rps-policy-primary			~
	Snapshot policy	important-ss-policy			~
	Backup policy	None			~
			Cancel	Add	

 輸入新的策略名稱、或輸入現有名稱以進行複製。如果您輸入現有名稱、請選擇要複製的名稱、然後選取 * 複製 *。



如果您選擇複製及修改現有策略、服務會將「 _copy 」附加至原始名稱。您應該變更名稱和 至少一個設定、使其成為唯一的。

- 5. 針對每個項目、選取*向下箭頭*。
 - [•] * 偵測政策 * :
 - •*原則*:選擇預先設計的偵測原則之一。
 - •*主要偵測*:啟用勒索軟體偵測功能、讓服務偵測可能的勒索軟體攻擊。
 - * 封鎖副檔名 * : 啟用此選項可讓服務封鎖已知可疑的副檔名。啟用主要偵測時、服務會自動擷取快 照複本。

如果您要變更封鎖的副檔名、請在 System Manager 中編輯副檔名。

[。]* Snapshot 原則 * :

- * * Snapshot 原則基礎名稱 * : 選取原則或選取 * Create * 並輸入快照原則的名稱。
- * Snapshot 鎖定 *: 啟用此選項可鎖定主儲存設備上的快照複本、即使勒索軟體攻擊管理其通往備 份儲存目的地的方式、仍無法在一段時間內修改或刪除快照複本。這也稱為 _immutable 儲存設備 _ 。如此可加快還原時間。

快照鎖定時、磁碟區過期時間會設為快照複本的到期時間。

ONTAP 9.12.1 及更新版本均提供 Snapshot 複本鎖定功能。若要深入瞭解 SnapLock 、請參閱 "ONTAP 中的 SnapLock"。

- * Snapshot 排程 * :選擇排程選項、要保留的快照複本數量、然後選取以啟用排程。
- 。* 備份原則 * :
 - * 備份原則基礎名稱 * : 輸入新名稱或選擇現有名稱。
 - •* 備份排程*:選擇次要儲存設備的排程選項並啟用排程。



若要在次要儲存設備上啟用備份鎖定、請使用 * 設定 * 選項來設定備份目的地。如需詳細資 訊、請參閱 "設定"。

6. 選取*「Add*」。

將偵測原則新增至已有快照和備份原則的工作負載

透過 BlueXP 勒索軟體保護、您可以將勒索軟體偵測原則指派給已有快照和備份原則的工作負載、這些原則是 在其他 NetApp 產品或服務中管理的。偵測原則不會變更在其他產品中管理的原則。

其他服務(例如 BlueXP 備份與還原及 SnapCenter)則使用下列類型的原則來管理工作負載:

- 管理快照的原則
- 管理複寫至次要儲存設備的原則
- 管理備份至物件儲存設備的原則

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。

0 16 Atink 0 404070	tays()		32 Gie Data at risk			7 Potech 1 (Last)	d D ays	14 Gið Deta protecte	¢		
Workfords		Protection grou	н								
(orkloads (24)									٩	4 Manage p	objection strategies
workload 9	type ====	Connector \$	Importance # \$	0 Macys. \$	Protection T	\$ Protection # \$	Detection * *	Detection _ T \$	Snapshot T \$	Backup desti 🗧	
Vm_datamore_useau	VM Ne share	ave-connector-us	pricel	69	Protected	eva.	Active	rps-policy-ad	Buell? (anomica	netapp-backup-vs	(Fox protection
Vm_dataction_convery	VM file share	ave-connector-us	Ortical	nia.	Protected	n/a	Learning mode	rpr-policy-all	Buel? lancomsa.,	netapp-backup-vs.,	(Inte protection
Vm_datastree_uswer	VM file share	ava convector us	Mandard	n/8	🛈 Atrisk	0.9	None	Note	None	nelapp-backup-vs	Profact
Virgilatastore.uswas	VM file share	ans connector-us	that-shared	e)/#	🛈 "Atrisk	n/a	None	None	Nore	netapp-backup-vs	Protect
Vm_datamore_useas	VM file share	ave-connector-us	Standard	n/a	() At the	0/3	None	None	Nore	netapp-backup-us	Protect
Vm datastone 201 3	VV for share	onprem-connecto	Sundard	n3	O Atrek	0/3	hone	hone	None	netapp-backsp-v6	Protect

2. 從「保護」頁面選取工作負載、然後選取*保護*。

「保護」頁面會顯示由 SnapCenter 軟體、 SnapCenter for VMware vSphere 和 BlueXP 備份與還原所管理 的原則。

下列範例顯示 SnapCenter 所管理的原則:

					ţ	Protect		
				Selec	t a detection policy to a	apply to th	e workload	i Oracle_9819.
Dete	ection policies (2)) 1 selected					a	Dicies managed by SnapCenter
	Name	🗢 Pri	mary detection	\$	Block suspicious file ex	tensions	\$	These policies managed by SnapCenter will not be modified by
0	rps-policy-1	Yes			Yes			applying a detection policy to this workload.
0	rps-policy-2	Yes			No			(b) ss-policy-daily1 Snapshot policy
								ss-policy-weekly1 Snapshot policy
								(a) ss-policy-weekly2 Snapshot policy
								ss-policy-monthly1 Snapshot policy
						_		
				1	Cancel	Pro	tect	

以下範例顯示 BlueXP 備份與還原所管理的原則:

			Protect	:		
			Select a detection policy to apply to	the workload My	/SQL_8009.	
Dete	ction policies (2)	1 selected		Q	Policies managed by BlueXP backup and recovery	
	Name	Primary detection	Block suspicious file extensions	÷	These policies managed by BlueXP backup and recovery will not be	
0	rps-policy-1	Yes	Yes		modified by applying a detection policy to this workload.	
0	rps-policy-2	Yes	No		(a) standart-snapshot-policy Snapshot policy	¢
					Standart-backup-policy Backup policy	
			Cancel	Protect		

- 3. 若要查看其他管理原則的詳細資料、請按一下*向下箭頭*。
- 4. 若要套用偵測原則、以及在其他地方管理的快照和備份原則、請選取偵測原則。
- 5. 選取*保護*。
- 在「保護」頁面上、檢閱「偵測原則」欄、查看指派的「偵測原則」。此外、快照和備份原則欄也會顯示管 理原則的產品或服務名稱。

指派不同的原則

您可以指派不同的保護原則來取代目前的保護原則。

步驟

- 1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
- 2. 從「保護」頁面的工作負載列中、選取*編輯保護*。
- 3. 在「原則」頁面中、按一下您要指派的原則向下箭頭、以檢閱詳細資料。
- 4. 選取您要指派的原則。
- 5. 選取 * 保護 * 以完成變更。

群組檔案共用以更容易保護

群組檔案共用可讓您更輕鬆地保護資料資產。此服務可同時保護群組中的所有磁碟區、而非分別保護每個磁碟 區。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。

0 16 Atriak () 4 Gar 7 6	tay-ti)		32 cie Data at risk			7 Potecke 1 gast 7	f Q dys	14 Gið Deta profeide	4		
Workfoads		Protection grou	р								
Workloads (24)									٩	4 Manage pro	tection strategas
Workload 8	type val	Consector 0	Importance # \$	O Mucys. :	Protection T 2	Protection T \$	Detection _ T 2	Detection _ T \$	Snapshot _ T \$	Backup desti 2	
Vm_datactore_useau	VM Ne share	ave-connector-us	pricel	n 9	Protected	69	Adhe	rps-policy-all	Build lanomika	netapp-backup-vs.,	(Fdt potenner)
Vm_datactive_unvery	VM file share	ava-connector-us	Ortical	na.	Protected	0/9	Learning mode	rpe-poley-ail	BuciP lancomika	netapp-backup-vs	(Retroverson)
Vm_datastime_unwer	vM file share	ives connector-us	Mandard	n/8	🛈 #tmk	n#	None	None	None	netapp-backup-vs	Protect
Virg datastine javwer	vM Ne share	ans connector-us	statulant	e)/#	🛈 "Atrisk	n/4	None	None	None	netapp-backup-vs	Protect
Vm_datamore_useas	VM-file share	ave-connector-us	Standard	n/a	() At the	n/a	None	None	None	netapp-backup-us	Protect
Ver datation, 201, 3	VVI file share	onprem-connecto	Sundard	na	C Atrick	n/a	None	hore	None	netapp-backup-vs	Protect

2. 從「保護」頁面中、選取 * 保護群組 * 索引標籤。

Atria () 4 has 7 deph		32.Gi6 Outs at mik	Protected @ 1 (Last T days)	14 GB Deta protected		
Workloads	Protection g	produ				
tection groups (1) Eproups to manage protects	or actors multiple workloads whi	ih uhan simlar charactaridics.			a Ŧ	Add
tection groups (1) I proups to manage protection Protection group	on actors multiple workloads whit Detection policy	ch share similar churacteristics:	T 2 Protection status	v 1 0 Protected count	Q ≟	A48

3. 選取*「Add*」。

Ransomware protection Add protection group					 Worksoads 	(2) Protection	3 Review			
					Select workload	Workloads is to add to the prot	iction group.			
	Protection group name protect-group-wyz					Select Workd	the type of workloads to sads with snapshot and napCenter or Backup an	add to the pr backup polici d recovery (otection group. es managed by 3 - Kansamware protecti	07
v	Norkloads (*	4) Z selected Worklaad	. 1	Type	¥2]	Connector	t i Importance	v 2	Privacy exposure	Q
v	Workloads (*	4) 2 selected Workload Oracle,9819	:	Type Oracle	w 2	Connector	¢ i Importance	*:	Privacy exposure 1/8	2 Protection status
v	Norkloads (*	4) 2 selected Workload Oracle_9819 Oracle_2115	:)	Type Oracle Oracle		Connector avis-connector-us-asst- avis-connector-us-asst-	Importance Important Important Important	*:	Privacy exposure 11/8 17/8	C Protection status Protected O Atmak
v	Norkloads (A) [2 selected Workload Oracle;9819 Oracle;2115 MySQL,9294	:)	Type Oracle Oracle MySQL		Connector ave connector-us-aust- ave-connector-us-aust-	Importance Important Important Critical	* :	 Privacy exposure n/a n/a 	 Protection status Protected At mik Protected

- 4. 輸入保護群組的名稱。
- 5. 請完成下列其中一個步驟:
 - a. 如果您已經有保護原則、請根據工作負載是否由下列其中一項管理、選擇是否要將其分組:
 - BlueXP 勒索軟體保護
 - SnapCenter 或 BlueXP 備份與還原
 - b. 如果您尚未制定保護原則、頁面會顯示預先設定的勒索軟體保護策略。
 - i. 選擇一個選項來保護您的群組、然後選取*下一步*。
 - ii. 如果您選擇的工作負載在多個工作環境中都有磁碟區、請選取多個工作環境的備份目的地、以便將 它們備份到雲端。
- 6. 選取要新增至群組的工作負載。



若要查看工作負載的詳細資料、請向右捲動。

7. 選擇*下一步*。

Add protection group	 Worklands 	Protection ③ Review		
		Protect		
	Select a detection policy to a	opply to all the workloads in the pro	Nection group.	
Detection policy (2) Selected rows (1)			SnapCenter and BlueXP backup and recovery	
Select Detection policy	Primary detection	Block suspicious file extensions	Existing snepshot and backup policies manaped by SnapCenter and BlackP backup and recovery will not be modified by applying	
rps-dietection-1	Xee	Yes	a detection policy to the salected workbads.	
rps-detection-7	Yes	No		
	Pres	NA		

8. 選取管理此群組保護的原則。

- 9. 選擇*下一步*。
- 10. 檢閱保護群組的選項。
- 11. 選取*「Add*」。

新增更多工作負載至群組

您稍後可能需要將更多工作負載新增至現有群組。

如果群組包含僅由 BlueXP 勒索軟體保護(而非由 SnapCenter 或 BlueXP 備份與還原管理)所管理的工作負載、則應針對僅由 BlueXP 勒索軟體保護所管理的工作負載、使用個別群組、而針對由其他服務管理的工作負

載、使用另一個群組。

步驟

- 1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
- 2. 從「保護」頁面中、選取*保護群組*索引標籤。

At mail () A frag 7 days;	32 Gi6 Outs at mik	Protec 1 (Lat	net © 14 Git 7 daysi Deta protect	iđ	
Workloads	Protection groups				
vitection groups (1) 31 groups to manage protection across mult	iple workloads which share similar characteridics.			۹ 🛓 🗖	Add
Protection group 2 Detection	policy = = = = = = = = = = = = = = = = = = =	icies T 2 Protection status	v 2 O Protected count	# 0 Backup destination	. 4

3. 選取您要新增更多工作負載的群組。

		b	p-dev-apps-group Protection group				
						Delete p	otection group
88 Workloads				0 /	rotection		dit protection
2 File stores	BB 0	cations	2 vivi datastores	۲	ps-policy all Protection group		
Workloads (4)					٩	±	- 44
Workloads (4) Workload C	Туре та	Connector 🗘	Importance V C (D Privacy exposure 🗧	Q Protection status	± Detection s	adat tata
Workloads (4) Workload ¢ vm_datastore_202_7359	Type # 2 VM datastore	Convector +	Importance v C (Dandard r	Privacy exposure I	Q Protection status © Protected	± Detection s Active	Add Lak
Workloads (4) Workload ÷ vm_datattore_202_7358 vm_datattore_203_3676	Yype T 2 VM datatore VM datatore	Convector ¢ : onprem-connector-accou	Importance T C (Standard r Important, r)): Privacy exposure 🗧 ca ya	Q Protection status = O Protected To as risk	± Detection I Active Tione	tati

4. 從選定的保護群組頁面中、選取*新增*。

BlueXP 勒索軟體保護功能只會顯示群組中尚未使用與群組相同快照和備份原則的工作負載。



頁面頂端會顯示維護快照、備份和偵測原則的服務。

- 5. 選取應新增至群組的其他工作負載。
- 6. 選擇*保存*。

編輯群組保護

您可以變更現有群組上的偵測原則。如果尚未將偵測原則新增至此群組、您可以立即新增。

步驟

- 1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
- 2. 從「保護」頁面中、選取*保護群組*索引標籤。

					fir	nance	-apps 🦉 nomun								
\$2 Workloads										0	Protec	tion		Delete protecti	ion gr
B 1 File starms			88	2 Applications		8	0 VM datastore			0) rps- Ram	-detection-1 somware detection	policy		
Workloads (3)													a.	±	Add
Worktoad	¢ 1	Type	₩\$ Ampo	tance 😤 🕻	O Privacy exposure T 2	Proto	ection wol	Deter statu	ntion =:	Detection policy	(# \$1	Snapshot and backup policies	¥\$1	Backup destination	ra I
oracle-app-01		Oracle	Critic	sí.	rite	0	Protected	0	Active	ros-detection-1		ShapCenter		AWS US East 10%	ēί.
fileshare_sourcest_03_0192		Fie share.	Critic	ы:	identify exposure	0	Protected	8	Error	rgin-detection-1		SnapCentar		AWS US East (ON	et.
practe-and-02		Docie -	1000	tabl	-	171	Protected	0	Active	rps-detection-1		SpapCenter		AWS US East 10N	

- 3. 從「保護」窗格中、選取*編輯保護*。
- 4. 選取或新增偵測原則至此群組。

移除群組中的工作負載

您稍後可能需要從現有群組移除工作負載。

步驟

- 1. 從 Blue XP 勒索軟體保護功能表中、選取 * 保護 * 。
- 2. 從「保護」頁面中、選取 * 保護群組 * 索引標籤。
- 3. 選取您要從中移除一或多個工作負載的群組。

econ > psp-dev-apps-group			bx	p-dev-apps-group Protection group				
							Delete pr	staction group
	22 Workloads				0 1	rotection		dit protection
	2 File shares	B8 0	ations	2 vtv datastores	۲	rps-policy-all Protection group		
	Workloads (4)					Q	±	
								(A11
	Workload \$	Type = =	Connector \$	Importance == = =	Privacy exposure I	Protection status	Detection a	ani
	Workload C	Type = = VM datastore	Connector \$	Importance == 0 Standard	Privacy exposure	Protection status :	Detection a	ant O
	Workload C vm_datastore_202_7359 ven_datastore_203_2576	Type T > 1 VM datastore VM datastore	Convector	Importance v t Randard Important	Privacy exposure I	Protection status Protected At risk	Detection a Active None	ati O

4. 在選定的保護群組頁面中、選取您要從群組中移除的工作負載、然後選取 * 動作 * ••• 選項。

- 5. 從「動作」功能表中、選取*移除工作負載*。
- 6. 確認您要移除工作負載、然後選取*移除*。

刪除保護群組

刪除保護群組會移除群組及其保護、但不會移除個別工作負載。

步驟

- 1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。
- 2. 從「保護」頁面中、選取*保護群組*索引標籤。
- 3. 選取您要從中移除一或多個工作負載的群組。

Protection 3 Exp-dev apps group			Ь	p-dev-apps-group				
							Delete p	otection group
	88 Workloads				0	Protection		dit profection
	2 File stares	0 Apple	ations	2 vvir datastories	0	ps-policy-all Protection group		
	Workloads (4)					Q	Ŧ	AM
	Workload C	Type T 2	Connector +	Importance == 0	Privacy exposure	Protection status	Detection a	uh
	vm_datastore_202_7359	VM datastore	onprem-connector-accou	Randard	n/a	Protected	Active	Θ
	vm_datadore_203_2676	VM datastore	onprem-connector-accou	important	n/a	() At risk	tione	Θ
	fileshare_useast_01	File share	ave-connector-us-east-1	Standard	n/a	1 At risk	None	Θ

4. 從選取的保護群組頁面右上角、選取*刪除保護群組*。

5. 確認您要刪除群組、然後選取*刪除*。

管理勒索軟體保護策略

您可以刪除勒索軟體策略。

檢視受勒索軟體保護策略保護的工作負載

刪除勒索軟體保護策略之前、您可能想要檢視哪些工作負載受到該策略的保護。

您可以從策略清單或編輯特定策略時、檢視工作負載。

檢視策略清單時的步驟

1. 從 Blue XP 勒索軟體保護功能表中、選取 * 保護 * 。

2. 從「保護」頁面選取*管理保護策略*。

勒索軟體保護策略頁面會顯示策略清單。

		Ransomware protection	1 strategies				
Ransomware protection strategies (4)				Q	<u>+</u>	Add	
Ransomware protection strategy	2 Sisapshot policy	2 Backup policy	2 Detection policy	Protected workloads	:		
sps-stratage-critical	critical-st-policy	critical-bu-policy	spt-policy-all	з		~	
rpi-strategy-important,	important to policy	important-bur policy	rps policy all	((4))		~	217
eps-drategy-standard	standard-to-policy	standard-bu-policy	rps-policy-all	0		~	244
RPS strategy 4	standard-ss-policy-344	standard burpolicy-344	rps-policy-all	0		\sim	•••
					Delete rolicy		

3. 在勒索軟體保護策略頁面的受保護工作負載欄中、按一下列結尾的向下箭頭。

刪除勒索軟體保護策略

您可以刪除目前未與任何工作負載相關聯的保護策略。

步驟

1. 從 BlueXP 勒索軟體保護功能表中、選取 * 保護 * 。

2. 從「保護」頁面選取*管理保護策略*。

3. 在「管理策略」頁面中、針對您要刪除的策略選取 * 動作 * ••• 選項。

4. 從「動作」功能表中、選取*刪除原則*。

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。