

Proteja las cargas de trabajo

BlueXP ransomware protection

NetApp October 07, 2024

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

Tabla de contenidos

Proteja las cargas de trabajo	1
Proteger cargas de trabajo con estrategias de ransomware	1

Proteja las cargas de trabajo

Proteger cargas de trabajo con estrategias de ransomware

Puedes proteger las cargas de trabajo contra ataques de ransomware completando las siguientes acciones mediante la protección contra ransomware de BlueXP.

- Habilite la protección coherente con las cargas de trabajo, que funciona con el software SnapCenter o el complemento SnapCenter para VMware vSphere.
- Cree o gestione estrategias de protección frente al ransomware, que incluyen políticas que cree para copias Snapshot, backups y protección frente al ransomware (conocidas como *políticas de detección*).
- Importe una estrategia y ajústela.
- Agrupe los recursos compartidos de archivos para que le resulte más fácil proteger las cargas de trabajo en lugar de protegerlas individualmente.
- Elimina una estrategia de protección contra ransomware.

*¿Qué servicios se utilizan en la protección? * Los siguientes servicios pueden utilizarse para gestionar las políticas de protección. La información sobre protección de estos servicios aparece en la protección contra ransomware de BlueXP :

- Backup y recuperación de BlueXP para recursos compartidos de archivos y recursos compartidos de archivos de equipos virtuales
- · SnapCenter para VMware para almacenes de datos de máquinas virtuales
- SnapCenter para Oracle y MySQL

Políticas de protección

Puede resultar útil revisar información sobre las políticas de protección que se pueden cambiar y qué tipos de políticas existen en una estrategia de protección.

¿Qué políticas de protección puedes cambiar?

Puede cambiar las políticas de protección en función de la protección de las cargas de trabajo que tenga:

- Las cargas de trabajo no están protegidas por aplicaciones NetApp: Estas cargas de trabajo no están gestionadas por SnapCenter, el complemento SnapCenter para VMware vSphere o la copia de seguridad y recuperación de BlueXP. Estas cargas de trabajo pueden tener copias Snapshot realizadas como parte de ONTAP u otros productos. Si existe protección de ONTAP FPolicy, puede cambiar la protección de FPolicy mediante ONTAP.
- Cargas de trabajo con protección existente de aplicaciones NetApp: Estas cargas de trabajo tienen políticas de copias de seguridad o instantáneas administradas por SnapCenter, SnapCenter para VMware vSphere o copias de seguridad y recuperación de BlueXP.
 - Si SnapCenter, SnapCenter para VMware o el sistema de backup y recuperación de datos de BlueXP gestionan las políticas de backup o Snapshot, seguirán siendo gestionadas por estas aplicaciones. Con la protección frente al ransomware de BlueXP, también puedes aplicar una política de detección de ransomware a esas cargas de trabajo.
 - Si la protección autónoma de ransomware (ARP) y FPolicy en ONTAP gestionan una política de detección de ransomware, esas cargas de trabajo estarán protegidas y seguirán gestionándolas por

ARP y FPolicy.

*¿Qué políticas se requieren en una estrategia de protección contra ransomware? *

Las siguientes políticas son necesarias en la estrategia de protección contra ransomware:

- Política de detección de ransomware
- · Política de Snapshot

No es necesaria una política de backup en la estrategia de protección frente a ransomware de BlueXP .

Mira la protección contra ransomware en una carga de trabajo

Uno de los primeros pasos para proteger las cargas de trabajo es visualizar las cargas de trabajo actuales y su estado de protección. Se pueden ver los siguientes tipos de cargas de trabajo:

- · Cargas de trabajo de aplicaciones
- · Cargas de trabajo de máquinas virtuales
- · Cargas de trabajo de recursos compartidos de archivos

Pasos

- 1. En la navegación izquierda de BlueXP, selecciona Protección > Protección contra ransomware.
- 2. Debe realizar una de las siguientes acciones:
 - En el panel Protección de datos del panel, seleccione Ver todo.
 - En el menú, selecciona Protección.

0 16 404971	lays()		32 cie Data at risk			7 Protects 1 (Last 7	d () d	14 Gið Deta protada	6		
Workfoada	v	Protection grou	я								
Vorkloads (24)									٩	1 Manage pro	tection strategies
workload =	type == =	Convector 🗧	Importance # 2	O Mixey =_ \$	Protection T 2	Protection # \$	Detection _ T \$	Detection T \$	Snapshot _ T \$	Backup desti 🗧	
Vm,datastrine.useau	VM Ne share	ave-connector-us	pricel	19	Protected	60	Adhe	rps-policy-all	Buol7 lanomika	netapp-backup-vs	(Fill potente
Vm_dataction_convery	VM file share	ave-connector-us	onical	n'a	Protected	6/9	Learning mode	rps-policy-all	Buci7 taniomisa.,	netapp-backup-vs.,	(Ant protects
vire, datastore, uswer	vM file share	ave convector-us.	standard	n/#	🛈 Atmik	n/8	None	None	None	netapp-backup-vs	Protect
Virg datastore jusives	vM Ne share	avs connector-us	Mahdard	n/a	🕚 Atrisk	n/a	None	None	None	netapp-backup-vs	Promot
Vm_datamore_useas	VM file share	ave-connector-us	Standard	n/a	() Atriak	n/a	None	None	Nore	netapp-backup-vs	Protect
Vin datation 201.3	vivi file share	ongrem-connecto	Sundard	na	() Atrisk	n/a	hone	None	None	netapp-backup-vs	Protect

3. En esta página, puede ver y cambiar los detalles de protección de la carga de trabajo.



Para las cargas de trabajo que ya poseen una política de protección con un servicio de backup y recuperación de datos de SnapCenter o BlueXP, no se puede editar la protección. Para estas cargas de trabajo, el ransomware de BlueXP permite la protección autónoma frente a ransomware o la protección de FPolicy si ya están activados en otros servicios. Más información sobre "Protección autónoma de ransomware", "Backup y recuperación de BlueXP"y "FPolicy de ONTAP".

Detalles de protección en la página Protection

En la página Protection, se muestra la siguiente información sobre la protección de cargas de trabajo:

Estado de protección: Una carga de trabajo puede mostrar uno de los siguientes estados de protección para indicar si se aplica o no una política:

- **Protegido**: Se aplica una política. ARP está habilitado en todos los volúmenes relacionados con la carga de trabajo.
- En riesgo: No se aplica ninguna política. Si una carga de trabajo no tiene activada una política de detección primaria, está «en riesgo» aunque tenga activada una política de instantáneas y de backup.
- En progreso: Se está aplicando una política pero aún no se ha completado.
- Fallo: Se aplica una política pero no funciona.

Estado de detección: Una carga de trabajo puede tener uno de los siguientes estados de detección de ransomware:

- **Aprendizaje**: Recientemente se asignó una política de detección de ransomware a la carga de trabajo y el servicio está escaneando cargas de trabajo.
- Activo: Se asigna una política de protección de detección de ransomware.
- No establecido: No se asigna una política de protección de detección de ransomware.
- Error: Se asignó una política de detección de ransomware, pero el servicio encontró un error.



Cuando se habilita la protección en la protección frente a ransomware de BlueXP, la detección de alertas y la generación de informes se inician después de que el estado de la política de detección de ransomware cambie del modo de aprendizaje al modo activo.

Política de detección: Aparece el nombre de la política de detección de ransomware, si se ha asignado una. Si la política de detección no se ha asignado, aparece N/A.

Políticas de instantáneas y copias de seguridad: Esta columna muestra las políticas de instantáneas y copias de seguridad aplicadas a la carga de trabajo y al producto o servicio que administra dichas políticas.

- Gestionado por SnapCenter
- · Gestionado por el plugin de SnapCenter para VMware vSphere
- · Gestionado por backup y recuperación de datos de BlueXP
- Nombre de la política de protección contra ransomware que rige las copias Snapshot y los backups
- Ninguno

Importancia de la carga de trabajo

La protección frente al ransomware de BlueXP asigna una importancia o prioridad a cada carga de trabajo durante la detección, en función de un análisis de cada carga de trabajo. La importancia de la carga de trabajo se determina en las siguientes frecuencias de snapshots:

- Crítico: Copias instantáneas tomadas más de 1 por hora (programa de protección altamente agresivo)
- Importante: Copias instantáneas tomadas menos de 1 por hora pero más de 1 por día
- Estándar: Copias instantáneas tomadas más de 1 por día

Políticas de detección predefinidas

Puedes elegir una de las siguientes políticas predefinidas de protección contra ransomware de BlueXP , que están alineadas con la importancia de la carga de trabajo:

Nivel de política	Snapshot	Frecuencia	Retención (días)	n.o de copias snapshot	Número máximo total de copias Snapshot
Política de carga	Cada trimestre	Cada 15 min	3	288	309
de trabajo crítica	Todos los días	Cada 1 días	14	14	309
	Semanal	Cada 1 semanas	35	5	309
	Mensual	Cada 30 días	60	2	309
Política de carga	Cada trimestre	Cada 30 minutos	3	144	165
de trabajo important	Todos los días	Cada 1 días	14	14	165
e	Semanal	Cada 1 semanas	35	5	165
	Mensual	Cada 30 días	60	2	165
Política de carga	Cada trimestre	Cada 30 min	3	72	93
de trabajo estándar	Todos los días	Cada 1 días	14	14	93
	Semanal	Cada 1 semanas	35	5	93
	Mensual	Cada 30 días	60	2	93

Habilite una protección coherente con las aplicaciones o las máquinas virtuales con SnapCenter

La habilitación de la protección coherente con la aplicación o las máquinas virtuales ayuda a proteger las cargas de trabajo de sus aplicaciones o máquinas virtuales de una forma coherente, lo que consigue un estado inactivo y consistente para evitar la pérdida potencial de datos posteriormente si es necesario la recuperación.

Este proceso inicia el registro del servidor de software de SnapCenter para aplicaciones o el plugin de SnapCenter para VMware vSphere para máquinas virtuales mediante el backup y la recuperación de BlueXP.

Después de habilitar la protección consistente con la carga de trabajo, podrás gestionar las estrategias de protección en la protección frente al ransomware de BlueXP. La estrategia de protección incluye la instantánea y las políticas de backup gestionadas en otras partes, junto con una política de detección de ransomware gestionada en la protección frente al ransomware de BlueXP.

Para obtener más información sobre el registro de SnapCenter o el plugin de SnapCenter para VMware vSphere mediante el backup y la recuperación de BlueXP, consulte la siguiente información:

- "Registre el software del servidor SnapCenter"
- "Registre el plugin de SnapCenter para VMware vSphere"

Pasos

- 1. En el menú de protección contra ransomware de BlueXP, selecciona Dashboard.
- 2. En el panel Recomendaciones, busque una de las siguientes recomendaciones y seleccione **Revisar y corregir**:
 - · Registrate Servidor SnapCenter disponible con BlueXP
 - Registre el plugin de SnapCenter para VMware vSphere (SCV) con BlueXP
- 3. Siga la información para registrar el host de SnapCenter o el plugin de SnapCenter para VMware vSphere con el backup y la recuperación de BlueXP.
- 4. Vuelve a la protección contra el ransomware de BlueXP.
- 5. En la protección contra ransomware de BlueXP, accede a la consola e inicia de nuevo el proceso de detección.
- 6. En Protección contra ransomware de BlueXP, selecciona **Protección** para ver la página Protección.
- 7. Revise los detalles de la columna Snapshot y backup policies de la página Protection para ver que las políticas se gestionan en otros lugares.

Añada una estrategia de protección contra ransomware

Puedes añadir una estrategia de protección contra ransomware a las cargas de trabajo. La forma de hacerlo depende de si ya existen políticas de Snapshot y backup:

- * Cree una estrategia de protección contra ransomware si no tiene instantáneas o políticas de copia de seguridad*. Si las copias Snapshot o las políticas de backup no existen en la carga de trabajo, puede crear una estrategia de protección contra ransomware, que puede incluir las siguientes políticas que crea en la protección contra ransomware de BlueXP :
 - · Política de Snapshot
 - · Política de backup
 - · Política de detección de ransomware
- Crear una política de detección para cargas de trabajo que ya tienen políticas de instantáneas y copias de seguridad, que se administran en otros productos o servicios de NetApp. La política de detección no cambiará las políticas gestionadas en otros productos.

Crear una estrategia de protección contra ransomware (si no tiene snapshots ni políticas de backup)

Si las copias Snapshot o las políticas de backup no existen en la carga de trabajo, puede crear una estrategia de protección contra ransomware, que puede incluir las siguientes políticas que crea en la protección contra ransomware de BlueXP :

- · Política de Snapshot
- · política de backup
- · Política de detección de ransomware

Pasos para crear una estrategia de protección contra el ransomware

1. En el menú de protección contra ransomware de BlueXP, selecciona Protección.

0 16 40471	(ays)		32 Giê Data at risk				7 Protected (2) 1 (Last 7 days) 14			4 GB ra protected					
Workfords		Protection grou	а												
Workloads (24)										٩	1	unage protection str	rata-gare		
workload \$	type ====	Connector 🔹	Importance # \$	0 macys \$	Protect	tion = ‡	Protection T \$	Detection T 2	Detection T 2	Snapshot _ T 2	Backup dest	- • 1			
Vm_datamore_useau	VM Ne share	ave-connector-us	princel	na.	0	Protected	69	Athe	rps-policy-ait	Buttle Lancomica	netapp-back	p-6. (101 pr	Marinan		
Wm_statastrine_convery	VM file share	ave-connector-us	Critical	nia.	0	Protected	n/o	Learning mode	rps-policy-all	Buel? (anomisa.,	netapp-back	prs. (180	ohietzan		
Vm, datastere, uswer	vM file share	ave convector us.	Mandard	n/8	0	4t risk	0.9	None	Note	None	netapp-back	#11_ (PH)	Anci)		
Vin_datastere_uswer	vM file share	avs connector-us	Mandand	e)/a	•	±† risk	n/a	Nore	None	None	netapp-back	@-VAP10	met.)		
Vm_datamore_useas	VM file share	ave-connector-us	Standard	n/a	0	Ad visik	n/a	tione	None	Nore	netapp-back	put. (Pro	(ten		
We datastone 201,3	VV file share	onprem-connecto	Standard	na	0	At risk	nia	None	None	None	netapp-back	prés (Pro	nect)		

2. En la página Protección, selecciona Administrar estrategias de protección.

Protection > Ranson	ware protection strategies												
				P	Ransomware protec	tion strate	gies						
	Ransomware protection strategies (I)							q	0.3	±		Add	
	Ransonware protection strategy	• 1	Snapshot policy	0.1	Backup policy	(4)	Detection policy	Protected workloads			÷1	э	
	rpi-thategy-ortical		anticel-ra-policy		oritical-bu-policy		rpe-policy-all	3				~	
	rpi-strategy-important		important-sz-policy		important-bu-policy		spi-policy-all	10				~ .	(
	rps-strategy-standard		standard-supplicy		standard bu policy		ips-policy-all	00				\sim	

3. En la página Estrategias de protección contra ransomware, selecciona Agregar.

Protection > Manage protection strategies > Add ransomware p	protection strategy								
			Add ransomware p	protection strategy					
	Ransomware protection strategy name RPS strategy 1	5		Copy from existing ransomware protection strategy No policy selected	다 Select				
	Detection policy	rps-policy-primary			~				
	Snapshot policy	important-ss-policy			~				
	Backup policy	None			~				
			Cancel	Add					

4. Introduzca un nuevo nombre de estrategia o introduzca un nombre existente para copiarlo. Si introduce un nombre existente, elija el que desea copiar y seleccione **Copiar**.



Si decide copiar y modificar una estrategia existente, el servicio agrega «_copy» al nombre original. Debe cambiar el nombre y al menos una configuración para que sea única.

- 5. Para cada elemento, seleccione la flecha abajo.
 - Política de detección:
 - Política: Elija una de las políticas de detección prediseñadas.
 - Detección primaria: Habilita la detección de ransomware para que el servicio detecte posibles ataques de ransomware.
 - Extensiones de archivo de bloque: Permite que este tenga el bloqueo de servicio conocido extensiones de archivo sospechosas. El servicio realiza copias Snapshot automatizadas cuando la detección primaria está habilitada.

Si desea cambiar las extensiones de archivo bloqueadas, edítelas en System Manager.

- Política de Snapshot:
 - Nombre base de la política de instantáneas: Seleccione una política o seleccione Crear e introduzca un nombre para la política de instantáneas.
 - Bloqueo de instantáneas: Permite que esto bloquee las copias instantáneas en el almacenamiento primario para que no se puedan modificar o eliminar durante un cierto período de tiempo, incluso si un ataque de ransomware se dirige al destino de almacenamiento de la copia de seguridad. Esto también se denomina *almacenamiento inmutable*. Esto permite acelerar el tiempo de restauración.

Cuando una snapshot está bloqueada, la hora de caducidad del volumen se establece en la hora de caducidad de la copia Snapshot.

ONTAP 9.12.1 y las versiones posteriores ofrecen el bloqueo de copias de SnapVault. Para obtener más información acerca de SnapLock, consulte "SnapLock en ONTAP".

- **Programaciones de instantáneas**: Elija las opciones de programación, el número de copias de instantáneas que desea conservar y seleccione habilitar la programación.
- Política de respaldo:
 - Backup policy basename: Introduce un nombre nuevo o elige un nombre existente.
 - Horarios de copia de seguridad: Elija opciones de programación para el almacenamiento secundario y habilite el horario.



Para habilitar el bloqueo de copia de seguridad en el almacenamiento secundario, configure sus destinos de copia de seguridad usando la opción **Settings**. Para obtener más información, consulte "Configurar ajustes".

6. Seleccione Agregar.

Añada una política de detección a las cargas de trabajo que ya tengan políticas de Snapshot y backup

Con la protección frente a ransomware de BlueXP, puedes asignar una política de detección de ransomware a cargas de trabajo que ya tengan políticas de backup y Snapshot que se gestionen en otros productos o

servicios de NetApp. La política de detección no cambiará las políticas gestionadas en otros productos.

Otros servicios, como el backup y recuperación de BlueXP y SnapCenter, usan los siguientes tipos de políticas para gobernar las cargas de trabajo:

- · Políticas que rigen las snapshots
- Normativas que rigen la replicación en el almacenamiento secundario
- Directivas que rigen los backups del almacenamiento de objetos

Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona Protección.

16 Atusk () 4 (Let 7)	lays)	32 Gi8 Data at risk					7 Protected 0 1 East 7 days			4		
Workfoads		Protection grou	н									
Workfoads (24)										٩	4 Manage p	objection strategies
Workload \$	type == =	Connector \$	Importance # \$	0 macys. :	Protect	tion = ‡	Protection T \$	Detection T 2	Detection T \$	Snapshot _ T 2	Backup desti 🗧	
Vm_datamore_uneour	VM Ne share	ave-connector-us	pricel	193	0	Protected	10	Adhe	rps-policy-adl	Buot lanomia	netapp-backup-vs	(FOR protection)
Vm_slatartime_uneer	VM file share	ain-connector-us	Critical	0.9	0	Protected	n,o	Learning mode	rps-policy-all	Buell? lansomeau	netapp-backup-vs	(Add protection)
Vm_datastere_sower	vM file share	ives connector-us	Standard	n/8	0	4t risk	n#	None	None	None	netapp-backup-is	Protect
Virg datastine jawes	vM Ne share	avis-convector-us	statulant	nja	•	at risk	n/4	Nore	None	None	netapp-backup-vs	Protect
Vm_datamore_useas	VM file share	ave-connector-us	Standard	0/3	0	Ad visik	n/a	None	None	None	netapp-backup-vs	Promet
Ver, datastow, 201,3	VV file share	onprem-connecto	Standard	nia	0	At risk	nia	None	None	None	netapp-backup-vs	Protect

2. En la página Protección, seleccione una carga de trabajo y seleccione Proteger.

La página Protect muestra las políticas gestionadas por el software de SnapCenter, SnapCenter para VMware vSphere y backup y recuperación de BlueXP.

El siguiente ejemplo muestra las políticas gestionadas por SnapCenter:

			Protect			
			Select a detection policy to apply to the	ne workload (Dracle_9819.	
Dete	ection policies (2) 1 selected		Q	Policies managed by SnapCenter	
	Name	Primary detection	ction 🗘 Block suspicious file extensions	÷	These policies managed by SnapCenter will not be modified by	
0	rps-policy-1	Yes	Yes		applying a detection policy to this workload.	
С	rps-policy-2	Yes	No		(b) ss-policy-daily1 Snapshot policy	~
					Snapshot policy	~
					Snapshot policy	~
					ss-policy-monthly1 Snapshot policy	~

En el siguiente ejemplo se muestran las políticas gestionadas por backup y recuperación de datos de BlueXP:

	Protect			
	Select a detection policy to apply to the v	orkload MySQL_800	Э.	
Detection policies (2) 1 selected	c	0	Policies managed by BlueXP backup and	recovery
Name 💠 Primary detection	Block suspicious file extensions	\$ These	e policies managed by BlueXP backup and reco	very will not be
S rps-policy-1 Yes	Yes	mod	fied by applying a detection policy to this work	load.
prps-policy-2 Yes	No	(1)	standart-snapshot-policy Snapshot policy	\sim
		6	standart-backup-policy Backup policy	~
	Greet			

- 3. Para ver los detalles de las políticas administradas en otro lugar, haga clic en la flecha abajo.
- 4. Para aplicar una política de detección además de las políticas de instantáneas y copias de seguridad gestionadas en otros lugares, seleccione la política de detección.
- 5. Seleccione Proteger.
- 6. En la página Protección, revise la columna Política de detección para ver la política de detección asignada. Además, la columna Instantánea y políticas de copia de seguridad muestra el nombre del producto o servicio que gestiona las políticas.

Asigne una política diferente

Puede asignar una política de protección diferente a la actual.

Pasos

- 1. En el menú de protección contra ransomware de BlueXP, selecciona Protección.
- 2. En la página Protección, en la fila de carga de trabajo, seleccione Editar protección.
- 3. En la página Policies, haga clic en la flecha hacia abajo de la política que desea asignar para revisar los detalles.
- 4. Seleccione la política que desea asignar.
- 5. Selecciona **Proteger** para finalizar el cambio.

Agrupe los recursos compartidos de archivos para una protección más sencilla

La agrupación de recursos compartidos de archivos facilita la protección del patrimonio de datos. El servicio puede proteger todos los volúmenes de un grupo a la vez, en lugar de proteger cada volumen por separado.

Pasos

1. En el menú de protección contra ransomware de BlueXP, selecciona Protección.

0 16 4 (Let T)	taya)		32 Gib Data at risk			7 Protecte 1 (Last 7	nd () 14 G8 7 days Deta potades						
Workfords		Protection grou	н (
(orkloade (24)									٩	4 Manage prof	ection strategies		
Workload 9	type va	Connector \$	Importance # \$	0 Macys_ 1	Protection # \$	Protection T \$	Detection T 2	Detection _ T \$	Snapshot T \$	Backup desti 🗧			
Vm_datastone_useau	VM Ne share	ave-connector-us	pricel	59	Protected	69	Active	rps-policy-ait	Build lanomika	netapp-backup-vs.,	Fill protection		
Vm datastrine unerer	VM file share	ans-connector-us	Ortical	n a	Protected	n,o	Learning mode	rps-policy-all	Buel? lanomia.	netapp-backup-vs.,	Rela proheima		
Vrs. datastore uswer	vM file share	ave connector-us	Mandard	n/8	🛈 4t mik	n%	None	None	None	netapp backup vs	Protect		
Virg datastore juwer	vM file share	ans connector-us	statulant	e)/a	🕐 Atrisk	n/4	None	None	None	netapp-backup-vs	Puttert		
Vm_datastore_useas	VM-file share	ave-connector-us	Standard	n/a	() Atritk	0/3	None	None	Nore	netapp-backup-vis	Protect		
Ven datastree, 201, 3	VV förshare	onprem-connecto	Standard	na	() Atrek	n/a	None	hore	None	netapp-backsp-v6	Putert		

2. En la página Protección, seleccione la pestaña Grupos de protección.

16 4 tate 7 Gent	32 Ga Outs at	s na		Protected (0) 1 guet 7 days		14 cm Deta protected			
Workloads	Protection groups						٥		44
Add groups to manage protection across in	sultiple workloads which share similar	dunderidici.					-	-	
Protection group C Detect	ton policy T 2	Snapshot and backup policies	(* 1)	Protection status	71 0 Pc	rtected count	₹ \$ Backup deit	inution	
hisp-dev appe group i ge po	icy-ell	SnapCenter		Protected	542.8		ant-st-det	1, avoid-dect-2	

3. Seleccione Agregar.

Ad @	nsonware protection dd protection group					Wörkösad	0 P	Hotection	3 Review				
						Select worklo	Workloa	ads the protection	i gravp.				
		Protection protect	group name group-rojz					Select the ty Workloads v ShapCi	pe of workloads to eith snapshot and enter or Backup an	add to the pr backup polici d recovery	otection group. es managed by Concurrence protection	91	
	w	forkloads	(4) 2 selected Workload	: 1	Туре	* :1	Connector	: 1	Importance	**	Privacy exposure	Q S Protection status	ĩ
			Oracle_9819		Oracle.		ava-connector	Superior Superior	Important		n/a	Protected	
			Oracle_2115		Oracle		aws-connector	-united to	Critical		nda	🕖 Atmik	
			MySQL_8294		MySQL		awi-connector	-us-east-1	Critical		eva.	Protected	
			MySQL_8009		MySQL		ave-connector	-ue-east-1-,	Çritical		n/a	🕖 Atria	
						1.5	Next	- 1					

- 4. Introduzca un nombre para el grupo de protección.
- 5. Realice uno de los siguientes pasos:
 - a. Si ya cuenta con políticas de protección, seleccione si desea agrupar cargas de trabajo según si las gestiona una de estas:
 - Protección contra ransomware de BlueXP
 - Backup y recuperación de datos de SnapCenter o BlueXP
 - b. Si ya no tienes políticas de protección implementadas, la página muestra las estrategias preconfiguradas de protección contra ransomware.
 - i. Elige uno para proteger tu grupo y selecciona Siguiente.
 - ii. Si la carga de trabajo que ha elegido tiene volúmenes en varios entornos de trabajo, seleccione el destino de backup para los múltiples entornos de trabajo para que se puedan hacer backups en el cloud.
- 6. Seleccione las cargas de trabajo que se añadirán al grupo.



Para ver más información sobre las cargas de trabajo, desplácese a la derecha.

7. Seleccione Siguiente.

			Select a detectio	n policy to ap	Protect	r protection gro	up.
Detection o	ulicy (3) 1 Selected mus (1	1					SnapCenter and BlueXP backup and recovery
Select	Detection policy	• 1	Primary detection	\$1	Bock suspicious file extensions	=)	Existing snapshot and backup policies managed by SnapCenter and BlackP backup and recovery will not be modified by applying
0	rps-detection-1		Yes		Yes		a detection policy to the salected workbarts.
0	rps-detection-2		Yes		No		

- 8. Seleccione la política que regirá la protección de este grupo.
- 9. Seleccione Siguiente.
- 10. Revise las selecciones del grupo de protección.
- 11. Seleccione Agregar.

Añada más cargas de trabajo a un grupo

Es posible que más adelante deba agregar más cargas de trabajo a un grupo existente.

Si el grupo incluye cargas de trabajo gestionadas solo mediante la protección contra ransomware de BlueXP (y no mediante el backup y recuperación de datos de SnapCenter o BlueXP), debería usar grupos separados para cargas de trabajo que gestionen solo con la protección contra ransomware de BlueXP y otro grupo para cargas de trabajo gestionadas por otros servicios.

- 1. En el menú de protección contra ransomware de BlueXP, selecciona Protección.
- 2. En la página Protección, seleccione la pestaña Grupos de protección.

0 10 At this, () 4 (Last 7 Gapt)	3.	2 G-6 ta at mik		Protected @ 1 Galet 7 days)	14 cas Deta protected		
Workloads	Protection groups	<u>]</u>					
ection groups (1) proups to manage protection acr	m multiple workloads which share si	niar dunchridics.				α¥	Add
		Snambot and backup redicter	(***)	Protection status	v 2 O Protected count	T 2 Backup destinution	. 4
notection group 🕴 D	stection policy T :						

3. Seleccione el grupo al que desea añadir más cargas de trabajo.

		b	xp-dev-apps-group Protection group			Delete pr	ofection group
88 Workloads				0	Protection	1	dit protection
2 File shares	BB 0	cations	2 vvi datastores	()	rps-policy-atl Protection group		
Workloads (4)					٩	±	All
Workloads (4) Workload C	Туре те	Connector \$	Importance == 0	Privacy exposure	Q. Protection status	±	ANI UR
Workloads (4) Workload C vm_datattore_202_7359	Type # 2 VAI datastore	Convector Conceptor account	Importance (# C Standard	Or Privacy exposure ÷ n/a	Q Protection status :	± Detection s Active	All un
Workloads (4) Workload Workload wm_datastore_202_7359 wm_datastore_203_2676	Type T C VM datastore VM datastore	Connector Connector accou- onprem-connector accou-	Importance	Philacy imposure ‡ n/a n/a	Q Protection status : Protected To at risk	± Detection s Active Trone	- AH

4. En la página del grupo de protección seleccionado, seleccione Agregar.

La protección frente a ransomware de BlueXP muestra que solo las cargas de trabajo que no se encuentran en el grupo que usan las mismas políticas de snapshot y backup que el grupo.



La parte superior de la página muestra qué servicio mantiene las políticas de instantánea, copia de seguridad y detección.

- 5. Seleccione las cargas de trabajo adicionales que se deben añadir al grupo.
- 6. Seleccione Guardar.

Editar protección de grupo

Puede cambiar la política de detección en un grupo existente. Si la política de detección aún no se ha agregado a este grupo, puede agregarla ahora.

- 1. En el menú de protección contra ransomware de BlueXP, selecciona Protección.
- 2. En la página Protección, seleccione la pestaña Grupos de protección.

on > Tenance-appe					fin Pro	ance	-apps 🖉						
												Delete protection	Brands
22 Workloads										O Protect	tion	tain der store	tion
1 File shares				2 Applications		8	0 VM datastore	i)		() rps-	detection-1 converse defection polic	r.	
Workloads (3)											٩	±	đ
Workload	01	Туре	¥\$1	Importance V :]	Privacy exposure ¥ :	Prote	ection wol	Deter statu	tion w:	Detection policy T \$	Snapshot and backup policies w :	Backup destination • :	:11
oracte-app-01		Oracle		Critical	n/a-	0	Protected	0	Active	rps-detection-3	ShapCenter	AWS US East 10Hits	(
fileshare_advent_03_0192		File share		Critical	identify exposure	Θ	Protected	8	Error	rps-detection-1	SnapCentar	AWS US East (ONc)	(
practe-app-02		Dade		important	nte	12	Protected	\odot	Active	tps-detection-1	SnapCenter	AWS US bast (ONic)	1

- 3. En el panel Protección, seleccione Editar protección.
- 4. Seleccione o agregue una política de detección a este grupo.

Quitar cargas de trabajo de un grupo

Es posible que más adelante deba eliminar cargas de trabajo de un grupo existente.

- 1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
- 2. En la página Protección, seleccione la pestaña Grupos de protección.
- 3. Seleccione el grupo del que desea quitar una o varias cargas de trabajo.

Protection > bxp-dev-apps-group								
			bx	p-dev-apps-group Protection group				
							Delete pr	otection group
	88 Workloads				0 1	rotection		dit protection
	<u> </u>	88 0		2	0	rps-policy-all Protection group		
	- T HE 3141 C3	- Abdree		The sector of the				
	Workloads (4)					Q	÷	AM
	Workload \$	Type T 2	Convector \$	Importance == 0	Privacy exposure	Protection status \$	Detection st	uti
	vm_datastore_202_7359	VM datastore	onprem-connector-accou	Standard	nja	Protected	Active	Θ
	vm_datastore_203_2676	VM datastore	onprem-connector-accou	Important	n/a	🛈 Atrick	tione	Θ
	fileshare_useast_01	File share	ave-connector-us-east-1	Standard	n/a	1 At risk	None	Θ

- 4. En la página del grupo de protección seleccionado, seleccione la carga de trabajo que desea eliminar del grupo y seleccione la opción *Acciones*....
- 5. En el menú Acciones, seleccione Eliminar carga de trabajo.
- 6. Confirme que desea eliminar la carga de trabajo y seleccione **Eliminar**.

Elimine el grupo de protección

Al eliminar el grupo de protección se quita el grupo y su protección, pero no se quitan las cargas de trabajo individuales.

Pasos

- 1. En el menú de protección contra ransomware de BlueXP, selecciona Protección.
- 2. En la página Protección, seleccione la pestaña Grupos de protección.
- 3. Seleccione el grupo del que desea quitar una o varias cargas de trabajo.



- 4. En la página del grupo de protección seleccionado, en la parte superior derecha, selecciona **Eliminar** grupo de protección.
- 5. Confirme que desea eliminar el grupo y seleccione Eliminar.

Gestionar las estrategias de protección frente al ransomware

Puedes eliminar una estrategia de ransomware.

Mira cargas de trabajo protegidas por una estrategia de protección frente al ransomware

Antes de eliminar una estrategia de protección contra ransomware, es posible que desee ver qué cargas de trabajo están protegidas por esa estrategia.

Puede ver las cargas de trabajo desde la lista de estrategias o cuando está editando una estrategia específica.

Pasos para ver la lista de estrategias

- 1. En el menú de protección contra ransomware de BlueXP, selecciona Protección.
- 2. En la página Protección, selecciona Administrar estrategias de protección.

La página Estrategias de protección contra ransomware muestra una lista de estrategias.

ection + Ra	Ransomware protection strategies										
	Ransomware protection strategies (4)				Q	±	Add	6			
	Ransomware protection strategy	Snapshot policy	2 Backup policy	C Detection policy	Protected workloads	:					
	spi-strategy-colocal	ottical-st-policy	critical-bu-policy	rpe-policy-all	з		~	***			
	epi-strategr-important.	important to policy	important-bu-policy	rps-policy-all	(91)		~	217			
	epi-diategy-standard	standard-to-policy	standard-bu-policy	rps-policy-all	0		~				
	775 strategy 4	standard-ss-policy-344	standard burgolicy-344	the policy all			\sim	***			
						till policy Delete policy					

3. En la página Ransomware protection Strategies, en la columna Protected Workloads, haga clic en la flecha hacia abajo al final de la fila.

Elimina una estrategia de protección contra ransomware

Es posible eliminar una estrategia de protección que actualmente no esté asociada a ninguna carga de trabajo.

- 1. En el menú de protección contra ransomware de BlueXP, selecciona **Protección**.
- 2. En la página Protección, selecciona Administrar estrategias de protección.
- 3. En la página Administrar estrategias, selecciona la opción **Acciones** para la estrategia que deseas eliminar.
- 4. En el menú Acciones, selecciona Eliminar política.

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.