

保护工作负载 BlueXP ransomware protection

NetApp October 07, 2024

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

目录

保护工作负载 · · · · · · · · · · · · · · · · · · ·	· · · · · · · · · · · · · · · · · ·	1
利用勒索软件策略保护工作负载······		1

保护工作负载

利用勒索软件策略保护工作负载

您可以通过使用BlueXP勒索软件保护完成以下操作来保护工作负载免受勒索软件攻击。

- 启用工作负载一致的保护、此功能可与适用于VMware vSphere的SnapCenter软件或SnapCenter插件结合使用。
- 创建或管理勒索软件保护策略、其中包括您为快照、备份和勒索软件保护创建的策略(称为_detection policies_)。
- 导入策略并进行调整。
- 对文件共享进行分组、使您可以更轻松地保护工作负载、而不是逐个进行保护。
- 删除勒索软件保护策略。

*哪些服务用于保护?*以下服务可用于管理保护策略。来自这些服务的保护信息显示在BlueXP 勒索软件保护中:

- •为文件共享、VM文件共享提供BlueXP 备份和恢复
- 适用于VMware的VM数据存储库SnapCenter
- •适用于Oracle和MySQL的SnapCenter

保护策略

您可能会发现、查看有关可以更改的保护策略以及保护策略中的策略类型的信息会很有帮助。

您可以更改哪些保护策略?

您可以根据所拥有的工作负载保护更改保护策略:

- 不受NetApp应用程序保护的工作负载:这些工作负载不受SnapCenter、适用于VMware vSphere 的SnapCenter插件或BlueXP 备份和恢复管理。这些工作负载可能会在ONTAP或其他产品中创建快照。如 果已启用ONTAP FPolicy保护、则可以使用ONTAP更改FPolicy保护。
- 受**NetApp**应用程序保护的工作负载:这些工作负载的备份或快照策略由SnapCenter、适用于VMware vSphere的SnapCenter或BlueXP 备份和恢复管理。
 - [•] 如果快照或备份策略由SnapCenter、SnapCenter for VMware或BlueXP 备份和恢复管理、则这些策略 将继续由这些应用程序管理。通过使用BlueXP 勒索软件保护、您还可以对这些工作负载应用勒索软件 检测策略。
 - [。]如果ONTAP中的勒索软件检测策略由自动勒索软件保护(ARP)和FPolicy管理、则这些工作负载将受到保 护、并将继续由ARP和FPolicy管理。

勒索软件保护策略需要哪些策略?

勒索软件保护策略需要以下策略:

• 勒索软件检测策略

• 快照策略

BlueXP 勒索软件保护策略不需要备份策略。

查看工作负载上的勒索软件保护

保护工作负载的第一步是查看当前工作负载及其保护状态。您可以看到以下类型的工作负载:

- 应用程序工作负载
- VM工作负载
- 文件共享工作负载
- 步骤
- 1. 从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。
- 2. 执行以下操作之一:
 - 。从信息板上的"Data Protection (数据保护)"窗格中、选择*查看全部*。
 - [。]从菜单中,选择*Protection。

16 Atriak (0) 404871	tays()		32 Git Data at risk				7 Protects 1 (Lest 7	d () d	14 GiB Deta protecte	6		
WorkSoads	v	Protection grou	pi I									
Workfoads (24)										٩	4 Manage pr	obection strategies
Workload =	type val	Connector 🔹	Importance T 2	O Musys. :	Prote	ction = ‡	Protection # \$	Detection _ T 2	Detection _ T \$	Snapshot _ T \$	Backup desti 🎗 🕴	
Weydatartow.useau	VM Ne share	avis-connector-us-	critical	na.	Ø	Protected	n/0	Athe	rps-policy-all	Bud? lanomia.	netapp-backup-vs	(Edit protection)
Vm_datactive_unvery	VM file share	ave-connector-us	critical	0.9	0	Protected	n/ə	Laaming mode	rps-policy-all	Suco lanomia	netapp-backup-vs	(Rela protection)
Vm, datastine uswer	vM file share	ave connector-us	Mandard	n/a	0		n/H	None	None	None	nelapp-balkup-vs	Protect
Viri, datastine Jower	vM Ne share	ans connector-us	statutant	e)/a	٢	At risk	n/4	None	Nore	tione	netapp-tackag-vs	Protect
Vm_datastore_useas	VM-file share	ave-connector-us	Standard	0/3	0	Abritik	0/3	tione	None	None	netapp-backup-vs	Protect
Vm datastow, 201, 3	VVI file share	onprem-convecto	Standard	na	0	Atrick	n/a	None	None	None	netapp-backup-vs	Putert

3. 在此页面中、您可以查看和更改工作负载的保护详细信息。

对于已使用SnapCenter或BlueXP备份和恢复服务制定保护策略的工作负载、您无法编辑此保 护。对于这些工作负载、如果已在其他服务中激活、则BlueXP勒索软件可启用自动勒索软件保护 和/或FPolicy保护。了解有关、和的更多信息 "自主勒索软件保护" "BlueXP备份和恢复" "ONTAP FPolicy"。

保护页面上的保护详细信息

 (\mathbf{i})

"Protection (保护)"页面显示了有关工作负载保护的以下信息:

保护状态:工作负载可以显示以下保护状态之一、以指示是否已应用策略:

- 受保护:应用策略。已在与工作负载相关的所有卷上启用ARP。
- •存在风险:未应用任何策略。如果工作负载未启用主检测策略、则即使启用了快照和备份策略、它也会处于"

风险"状态。

- •进行中:正在应用策略、但尚未完成。
- *failed *: 已应用策略,但策略不起作用。

检测状态:工作负载可以具有以下勒索软件检测状态之一:

- •正在学习:最近为工作负载分配了勒索软件检测策略、服务正在扫描工作负载。
- · Active: 已分配勒索软件检测保护策略。
- •未设置:未分配勒索软件检测保护策略。
- •错误:已分配勒索软件检测策略,但服务遇到错误。

 $\left(\begin{array}{c} \mathbf{Q} \end{array} \right)$

在BlueXP 勒索软件保护中启用保护后、在勒索软件检测策略状态从"学习"模式更改为"活动" 模式后、将开始进行警报检测和报告。

检测策略:如果已分配勒索软件检测策略、则会显示该策略的名称。如果尚未分配检测策略、则会显示"N/A"。 快照和备份策略:此列显示应用于工作负载以及管理这些策略的产品或服务的快照和备份策略。

- 由SnapCenter管理
- 由适用于VMware vSphere的SnapCenter插件管理
- 由BlueXP备份和恢复管理
- 用于管理快照和备份的勒索软件保护策略的名称
- 无

工作负载重要性

在发现期间、BlueXP勒索软件保护会根据对每个工作负载的分析为每个工作负载分配一个重要性或优先级。工作负载的重要性取决于以下快照频率:

- •严重:每小时创建1个以上的Snapshot副本(主动保护计划)
- 重要:每小时创建的Snapshot副本少于1个、但每天创建的Snapshot副本多于1个
- •标准:每天创建1个以上的Snapshot副本

预定义检测策略

您可以根据工作负载的重要性选择以下BlueXP 勒索软件保护预定义策略之一:

策略级别	Snapshot	Frequency	保留(天)	Snapshot副本数	Snapshot副本的 最大总数
关键工作 负载策略	每季度	每15分钟	3.	288	309
	每天	每1天	14	14	309
	每周	每1周	35	5.	309
	每月	每30天	60	2.	309
重要的工 作负载策	每季度	每30分钟	3.	144.	165
略	每天	每1天	14	14	165
	每周	每1周	35	5.	165
	每月	每30天	60	2.	165
标准工作 负载策略	每季度	每30分钟	3.	72.	93
	每天	每1天	14	14	93
	每周	每1周	35	5.	93
	每月	每30天	60	2.	93

利用SnapCenter实现应用程序或VM一致的保护

启用应用程序或VM一致的保护有助于您以一致的方式保护应用程序或VM工作负载、从而实现稳定一致的状态、 以避免日后需要恢复时可能丢失数据。

此过程将开始使用BlueXP备份和恢复为应用程序注册SnapCenter软件服务器或为VM注册适用于VMware vSphere的SnapCenter插件。

启用工作负载一致的保护后、您可以在BlueXP勒索软件保护中管理保护策略。保护策略包括在其他位置管理的 快照和备份策略、以及在BlueXP 勒索软件保护中管理的勒索软件检测策略。

要了解有关使用BlueXP备份和恢复注册适用于VMware vSphere的SnapCenter或SnapCenter插件的信息、请参阅以下信息:

- "注册SnapCenter服务器软件"
- "注册适用于VMware vSphere的SnapCenter 插件"

步骤

1. 从BlueXP勒索软件保护菜单中、选择*信息板*。

- 2. 从"建议"窗格中,找到以下建议之一,然后选择*复查并修复*:
 - 。向BlueXP注册可用的SnapCenter服务器
 - 。向BlueXP注册适用于VMware vSphere的SnapCenter插件(SCV)
- 3. 按照信息使用BlueXP备份和恢复注册适用于VMware vSphere的SnapCenter或SnapCenter插件主机。
- 4. 返回到BlueXP勒索软件保护。
- 5. 从BlueXP勒索软件保护中、转到信息板并重新启动发现过程。
- 6. 从BlueXP勒索软件保护中选择*保护*以查看保护页面。
- 7. 查看保护页面上的快照和备份策略列中的详细信息、以查看这些策略是否在其他位置进行管理。

添加勒索软件保护策略

您可以为工作负载添加勒索软件保护策略。执行此操作的方式取决于Snapshot和备份策略是否已存在:

- 如果没有快照或备份策略,请创建勒索软件保护策略。如果工作负载上不存在快照或备份策略、您可以创建 勒索软件保护策略、其中可包括在BlueXP 勒索软件保护中创建的以下策略:
 - 。快照策略
 - 。备份策略
 - 。勒索软件检测策略
- •*为已经具有快照和备份策略*的工作负载创建检测策略,这些工作负载在其他NetApp产品或服务中进行管理。检测策略不会更改在其他产品中管理的策略。

制定勒索软件保护策略(如果您没有快照或备份策略)

如果工作负载上不存在快照或备份策略、您可以创建勒索软件保护策略、其中可包括在BlueXP 勒索软件保护中 创建的以下策略:

- 快照策略
- 备份策略
- 勒索软件检测策略

制定勒索软件保护策略的步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。

0 16 4 Cast T	taya)		32 Gië Data at risk				7 Pictuche 1 (Last 7	f Q diye	14 Gið Deta protecte	e		
Workfoads		Protection grou	н									
Norkloads (24)										٩	1 Manage p	robection strategies
Workload 8	type =====	Convector 0	Importance # \$	O Maxye_ 1	Protec	ction = ‡	Protection T \$	Detection _ T 2	Detection _ T \$	Snapshot _ T 2	Backup desti 2	
Vm_datactore_useau	VM Ne share	ave-connector-us	pricel	19	٢	Protected	69	Adve	rps-policy-all	Buell? (anomica	netapp-backup-vs	(Fot potenting)
Vm_datactore_uneer	VM file share	avis-connector-us	Ortical	nia.	0	Protected	e/a	Learning mode	rpr-policy-all	Buell? cansomisa	retapp-backup-vs.,	(Ret protection)
Vin, datastime, uswer	vM file share	ave connector us.	Mandard	e/8	0	At risk	n/#	None	None	None	netapp-backup-vs	Protect
Virg distantione justives	vM file share	avs connector-us	Mahdard	e/a	٢	At risk	n/a	None	Nore	None	netapp-backup-vs	Protect
Vm_datamore_useas	VM file share	ave-connector-us	Standard	n/a	0	At visk	n/a	None	None	Nore	netapp-backup-vis	Protect
Very distantioner, 201, 3	VV file share	onprem-connecto	Standard	na	0	Atrek	n/a	None	hore	None	netapp-backup-vs	Protect

2. 在保护页面中,选择*管理保护策略*。

Protection > Ransor	ware protection strategies										
					Ransomware protec	tion strate	gies				
	Ransomware protection strategies (I)							c	i ±	Add	
	Ransomware protection strategy	* 1	Snapshot policy	<u>ः</u>	Backup policy	. • :	Detection policy	 Protected workloads		 	
	rpi-mategy-ortical		anticel-rangeology		ortical-bu-policy		rpe-policy-all	1		\sim	
	spi-shalogy-important		important-sc-policy		important-bu-policy		rps-policy-all	t)		\sim	(199)
	rpu-strategy-standard		standard-sepolicy		standard burgoticy		tps-policy-all	00		\sim	
	rps-strategy-standard		standard sirpolicy		(tandard bu-policy		(ps-policy-all	0 ()		~	- 1940

3. 从"RansU要 软件保护策略"页面中、选择*添加*。

Protection > Manage protection strategies > Add ransomware	protection strategy		Add ransomware p	protection strategy	
	Ransomware protection strategy name RPS strategy 1	2		Copy from existing ransomware protection strategy No policy selected	D Select
	Detection policy	rps-policy-primary			~
	Snapshot policy	important-ss-policy			~
	Backup policy	None			~
			Cancel	Add	

输入新的策略名称、或者输入现有名称进行复制。如果输入现有名称,请选择要复制的名称,然后选择*Copy*。



如果选择复制和修改现有策略、则该服务会在原始名称后附加"_copy"。您应更改此名称以及 至少一个设置、以使其唯一。

- 5. 对于每个项目,选择*向下箭头*。
 - 。检测策略:
 - •策略:选择预先设计的检测策略之一。
 - 主要检测: 启用勒索软件检测、使服务检测潜在的勒索软件攻击。
 - 阻止文件扩展名: 启用此选项可使服务阻止已知的可疑文件扩展名。启用主检测后、该服务会自动 创建Snapshot副本。

如果要更改阻止的文件扩展名、请在System Manager中编辑它们。

- [°] Snapshot策略:
 - * Snapshot policy base ame: 选择一个策略或选择*Create*并输入快照策略的名称。
 - Snapshot锁定: 启用此选项可锁定主存储上的Snapshot副本、以便在一段时间内无法修改或删除这些副本、即使勒索软件攻击设法到达备份存储目标也是如此。这也称为_immutable storage_。这样可以缩短恢复时间。

锁定快照后、卷到期时间将设置为快照副本的到期时间。

ONTAP 9.12.1及更高版本提供了Snapshot副本锁定功能。要了解有关SnapLock的更多信息、请参见 "ONTAP中的SnapLock"。

- * Snapshot计划:选择计划选项、要保留的Snapshot副本数、然后选择以启用计划。
- 。备份策略:
 - 备份策略基本名称: 输入新名称或选择现有名称。
 - 备份计划:为二级存储选择计划选项并启用计划。

要在二级存储上启用备份锁定,请使用*Settings*选项配置备份目标。有关详细信息,请参见 "配置设置"。

6. 选择 * 添加 * 。

向已具有Snapshot和备份策略的工作负载添加检测策略

借助BlueXP 勒索软件保护、您可以将勒索软件检测策略分配给已具有Snapshot和备份策略的工作负载、这些策略将在其他NetApp产品或服务中进行管理。检测策略不会更改在其他产品中管理的策略。

BlueXP备份和恢复以及SnapCenter等其他服务使用以下类型的策略来管理工作负载:

- 用于管理快照的策略
- 用于控制复制到二级存储的策略
- 用于管理对象存储备份的策略

步骤

 $[\]bigcirc$

1. 从BlueXP勒索软件保护菜单中、选择*保护*。

16 At Hick O 4 Gast To	taya)		32 GiB Data at risk				7 Protected 1 (Last 7	(Q Daye	14 Giß Data protactae	e ::		
Workfords		Protection grou	н									
Workfoads (24)										٩	4 Manage p	roboction strategies
workload = 1	type ====	Consector 0	Importance # \$	0 Macys. 1	Protecti	on = ‡	Protection_ T \$	Detection_ T +	Detection _ T \$	Snapshot _ = = =	Backup desti \$	
Vm,datartore.uneau	VM Ne share	ave-connector-us	oncel	59	() e	rotected	6/9	Athe	rps-policy-all	Build lanomika.	netapp-backup-vs.,	(Fex potenties)
Vm_datactive_conver	VM file share	ave-connector-us	Ontical	n a	() P	rotected	0,9	Learning mode	rps-policy-all	Buel? lanomia.	netapp-backup-vs.,	(Let prohetaan)
Vm_datastore_uswer	vM file share	ives convector-us	Standard	n/a	0 .	t risk	n/#	None	None	None	netapp-backup-vs	Protect
Vin_datastore_uswer	vM Ne share	ani (creatti-us	Statulard	nja	•	t risk	n/a	None	None	Note	netapp-tackup-vi	Puttert
Vm_datamere_useas	VM file share	ave-connector-us	Standard	n/a	0	t visk	n/a	None	None	None	netapp-backup-vs	Promet
Vendatantow, 201, 3	VVI file share	onprem-connecto	Standard	na	0	trok	n/s	none	hore	None	netapp-badsgrv6	Putert

2. 从保护页面中、选择一个工作负载、然后选择*保护*。

保护页面显示了由SnapCenter软件、适用于VMware vSphere的SnapCenter以及BlueXP备份和恢复管理的 策略。

以下示例显示了由SnapCenter管理的策略:

Detection	policies (2) 1 selec	Sele	ect a detection policy to apply to t	he workload Ora	cle_9819.	
Detection	policies (2) 1 selec					
		ted		Q	Policies managed by SnapCenter	
Na	me 🗘	Primary detection 💲	Block suspicious file extensions	÷	These policies managed by SnapCenter will not be modified by	
orps	-policy-1	Yes	Yes		applying a detection policy to this workload.	
) rps	-policy-2	Yes	No		ss-policy-daily1 Snapshot policy	~
					(ss-policy-weekly) Snapshot policy	~
					ss-policy-weekly2 Snapshot policy	~
					ss-policy-monthly1 Snapshot policy	~

以下示例显示了由BlueXP备份和恢复管理的策略:

	Protect		
	Select a detection policy to apply to the	e workload MyS	GQL_8009.
Detection policies (2) 1 selected		٩	Dolicies managed by BlueXP backup and recovery
Name 💠 Primary detection	on 🗘 Block suspicious file extensions	÷	These policies managed by BlueXP backup and recovery will not be
vps-policy-1 Yes	Yes		modified by applying a detection policy to this workload,
rps-policy-2 Yes	No		(a) standart-snapshot-policy Snapshot policy
			standart-backup-policy Backup policy
	Cancel	otect	

- 3. 要查看在其他位置管理的策略的详细信息,请单击*向下箭头*。
- 4. 要应用检测策略以及在其他位置管理的快照和备份策略、请选择检测策略。
- 5. 选择*保护*。
- 在保护页面上、查看检测策略列以查看分配的检测策略。此外、快照和备份策略列会显示管理策略的产品或 服务的名称。

分配其他策略

您可以分配不同的保护策略来替换当前保护策略。

步骤

- 1. 从BlueXP勒索软件保护菜单中、选择*保护*。
- 2. 从"Protection (保护)"页面的"Workload (工作负载)"行中、选择*编辑保护*。
- 3. 在策略页面中、单击要分配的策略对应的向下箭头以查看详细信息。
- 4. 选择要分配的策略。
- 5. 选择*保护*以完成更改。

对文件共享进行分组、以简化保护

通过对文件共享进行分组、可以更轻松地保护数据资产。该服务可以同时保护组中的所有卷、而不是单独保护每 个卷。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。

0 16 At Hilk O 4 Gast To	taya)j		32 cite Data at risk				7 Protecte 1 (Let 7	deys	14 Giß Data protecte	6		
WorkSoada		Protection grou	р									
Workfoads (24)										٩	1 Manage p	obection strategies
workload 9-1	type v a	Connector 0	Importance # \$	0 Maxys. 1	Protecti	on = ‡	Protection_ T \$	Detection_ T \$	Detection _ T \$	Snapshot _ T \$	Backup desti 🎗	
Vm_datactore_uneau	VM Ne share	ave-connector-us	priscal	69	() n	rotected	6,9	Active	rps-policy-all	Build lanomika	netapp-backup-vs.,	(Fdt protection)
Vm_datactive_uneer	VM file share	ava-connector-us	Critical	n a	() P	rotected	0/9	Laaming mode	rps-policy-all	Buell? lansomeau	retapp-backup-vs	(Ret protection)
Vm, datastine_uswei	vM file share	ans convector-us	Mandard	n/8	•	t risk	n/H	None	None	None	nelapp-backup-vs	(Profact)
Vir_datastore_uswes	vM Ne share	ans connector-us	Statulant	e)/#	() ·	t risk	n/a	None	None	Note	netapp-backup-vs	Protect
Vm_datastore_useas	VM-file share	ave-connector-us	Standard	n/a		t visk	n/a	None	None	None	netapp-backup-vic	Protect
Ven datastore 201.1	VVI file share	onprem-connecto	Sundard	na	0 .	trok	n/a	None	None	None	netapp-backup-vs	Putert

2. 从保护页面中,选择*保护组*选项卡。

16 At that 0 4 (Last 7 Gapt)		32 Gill Outra at mile	Protected () 1 filled T days	14 G.B Si Dela protected		
Workloads	Protection groups					
tection groups (1) proups to manage protection ac	on multiple workloads which share	n iimliir durachridics.			Q 1	Add
tection groups (1) (poups to manage protection ac Protection group 2 0	on multiple workloads which shar effection policy	n similar characteristics.	(₩.\$) Protection status	v 1 O Protected count	Q ±	Add T

3. 选择 * 添加 * 。

Ransonware protection Add protection group					 Workfoad 	2 Protecti	on	3 Review			
					Select workloa	Workloads do to add to the pro	stection (group.			
	Protection g	poup name poup xyz				Selec Worl	ct the type kloads wit SnapCen	t of workloads to th snapshot and ter or Backup an	add to the p backup polic d recovery	ntitection group. les managed by Consumware protect	891
v	Norkloads (*	4) 2 selected Workload	. 1	Type	v 0)	Connector		Importance	*1	© Privacy exposure	¢ i Protection status
v	Norkloada (*	4) 2 selected Workload Oracle_9815	• (Type Oracle	* 0	Connector .	¢.).	Importance Important	*:	Privacy exposure 1/8	C i Protection status
v	Workloads ()	4) [2 selected Workland Oracle_9819 Oracle_2115	• 1	Type Oracle Oracle	. ∀ \$.]	Connector aver-connector-us-eas aver-connector-us-eas	* Pts Nts	Importance Important Critical	*:	 Privacy supposure n/a 	2 Protection status C Protected () Atmak
	Norkloads (4) 2 selected Workload Oracle;9819 Oracle;2115 MySQL,8294		Type Oracle Oracle MySQL	. ≭ ≢.)	Connector avs-connector-us-eas avs-connector-us-eas	\$ 61 61	Importance Important Critical	* 2	Prhacy exposure //a //a //a	2 Modection status Protected 1 Armik Protected

- 4. 输入保护组的名称。
- 5. 完成以下步骤之一:
 - a. 如果您已制定保护策略、请选择是否要根据工作负载是否受以下策略之一管理对其进行分组:
 - BlueXP勒索软件保护
 - SnapCenter或BlueXP 备份和恢复
 - b. 如果您尚未制定保护策略、此页面将显示预配置的勒索软件保护策略。
 - i. 选择一个以保护您的组,然后选择*下一步*。
 - ii. 如果您选择的工作负载的卷位于多个工作环境中、请为多个工作环境选择备份目标、以便将其备份 到云。
- 6. 选择要添加到组中的工作负载。



7. 选择*下一步*。

Add protection gro	up		⊙ Wer	Noeds (Protection ③ Review	6		
			Select a detactio	n policy to ap	Protect	protection gro	up.	
							SnapCenter and BlueXP backup and recovery	
Detection po	Acy (2) Selected rows	(1)		- 20	Block suspicious file	Q	Existing snapshif and backup policies managed by SnapCenter	
Select	rps-detection-1	÷1 1	fee	÷	extensions Yes	÷.	and Black# backup and recovery will not be modified by applying a detection policy to the salected workloads.	
0	rps-detection-2		Ten .		No			
				Previo		i.		

8. 选择要管理此组的保护的策略。

- 9. 选择*下一步*。
- 10. 查看为保护组选择的内容。
- 11. 选择 * 添加 * 。

向组添加更多工作负载

您稍后可能需要向现有组添加更多工作负载。

如果该组中的工作负载仅由BlueXP 勒索软件保护管理(而不是由SnapCenter或BlueXP 备份和恢复管理)、则应 对仅由BlueXP 勒索软件保护管理的工作负载使用单独的组、而对由其他服务管理的工作负载使用另一组。

- 1. 从BlueXP勒索软件保护菜单中、选择*保护*。
- 2. 从保护页面中,选择*保护组*选项卡。

16 At mat. (0) 4 (Last 7 Gays)	32 Gi6 Outs at mik		Protected () 1 6.4et T daysi	14 GB Deta protected	
Workloads	Protection groups				
interfine county (T)					Q 1 AU
to proups to manage protection across m	itiple workloads which share similar charac	cleridica.			
M groups to manage protection across m Protection group 2 Detection	itiple workloads which share similar charac in policy == 2	cheridics. pathot and backup policies T 2	Protection status W	2 Ø Protected count	π 2 Radup detination - 1

3. 选择要添加更多工作负载的组。

		bx	p-dev-apps-group Protection group				
						Delete p	otection group
88 Workloads				Q P	otection		all polyclion
2 File shares	BB 0	ications	2 vtv datastories	0	rps-policy-all Protection group		
Workloads (4)					a	*	444
Workloads (4) Workload ¢	Type T C	Connector \$	Importance V C 0): Privacy exposure 💲	Q.	± Detection (add tab
Workloads (4) Workload C vm_datattore_202_7359	1 Type = 2 VM datatione	Connector + onprem-connector-accou.	Importance == 0 6 Standard n)Privacy exposure 💲	Q Protection status *	± Detection s Active	Add tath
Workloads (4) Workload wm_datastore_202_7359 wm_datastore_203_2576	VM datastore	Convector 2 1 conprem-convector-accou	Importance TO ()	8 Privacy exposure \$ cs	Q. Protection status Protected T At risk	± Detection : Active None	441 tak (-)

4. 从"Selected protection group"(选定保护组)页面中、选择*Add*。

BlueXP 勒索软件保护仅会显示组中尚未使用与组相同的快照和备份策略的工作负载。



页面顶部显示了维护快照、备份和检测策略的服务。

- 5. 选择应添加到组中的其他工作负载。
- 6. 选择*保存*。

编辑组保护

您可以更改现有组上的检测策略。如果检测策略尚未添加到此组、则可以立即添加它。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。

2. 从保护页面中,选择*保护组*选项卡。

			fin er	iance-apps 🖉					
								Delete protection (pa
22 Workloada						O Protec	tion	Editoretech	on
1 File stares		2 Applications		0 VM datastore		() rps Ran	detection-1 somware detection policy		
Workloads (3)							٩	1 Add	
Workload] Type	♥\$ Importance ₹\$]	Privacy exposure T	Protection w \$	Detection w t status	Detection policy Ψ \$ [Snapshot and backup policies # :	Backup destination = 1	ľ
oracte-app-01	Oracie	Critical	N/#	Protected	 Active 	rps-detection-1	ShapCentor	AWS US East 10%its	1
fileshare_uswest_03_0192	Fie share.	Critical	identify exposure	Protected	Erner	run-detection-1	SnapCentar	AWS US East (ONc)	1
practe-app-02	Dade	important	n/a	Protected	Active	tps-detection-1	ShapCenter	AWS US East IONICI	1

- 3. 从保护窗格中,选择*编辑保护*。
- 4. 选择检测策略或将其添加到此组。

从组中删除工作负载

您稍后可能需要从现有组中删除工作负载。

步骤

- 1. 从BlueXP勒索软件保护菜单中、选择*保护*。
- 2. 从保护页面中,选择*保护组*选项卡。
- 3. 选择要从中删除一个或多个工作负载的组。

Protection 3 http-dev apps-group			bx	p-dev-apps-group Protection group				
							Delete pro	stedion group
	88 Workloads				0 /	rotection		dit profection
	2 File stares	0 apple	ations	2 vtv datastores	۲) rps-policy-all Protection group		
	Workloads (4)					Q	£	-
	Workload \$	Туре — = =	Convector \$	Importance T C	Privacy exposure	Protection status	Detection st	ah
	vm_datastore_202_7359	VM datastore	onprem-connector-accou	Standard	n/a	Protected	Active	Θ
	vm_datatione_203_3676	VM datastore	onprem-connector-accou	important	n/a	() Atrick	None	Θ
4	fileshare_useast_01	File share	ave-connector-ve-east-1	Standard	nya -	① At resk	None	Θ

4. 从"Selected protection group"(选定保护组)页面中、选择要从组中删除的工作负载、然后选择*操作*---选项。

- 5. 从操作菜单中,选择*Remove Workload*。
- 6. 确认要删除此工作负载,然后选择*Remove*。

删除此保护组

删除保护组将删除该组及其保护、但不会删除各个工作负载。

步骤

- 1. 从BlueXP勒索软件保护菜单中、选择*保护*。
- 2. 从保护页面中,选择*保护组*选项卡。
- 3. 选择要从中删除一个或多个工作负载的组。

			Protection group				
						Delete pr	otection group
88 Workloads				0	Protection		chit protection
2 File stores	B8 0	cations	2 vvv datastores	0) rps-policy-all Protection group		
Workloads (4)					٩	±	AN
Workloads (4) Workload C (Туре та	Convector \$	Importance T 5 (Privacy exposure ‡	Q. Protection status	±	ANI Lat
Workloads (4) Workload C (vm_datastore_202_7359	Nype # 2 VM datatore	Convector C onpremiconnector-accou.	Importance T C (Standard)	D: Privacy exposure 🗢	Q Protection status	± Detection at Active	anti tati
Workloads (4) Workload C (vm_datatore_202_7359 vm_datatore_203_3676	Type Tr C VM datatione VM datatione	Connector +	i Importance v C (Standard r Important r	Privacy exposure I	Q Protection status Protected () At risk	± Detection at Active Trone	AH on O

4. 从选定保护组页面的右上角选择*删除保护组*。

5. 确认要删除该组,然后选择*Delete*。

管理勒索软件保护策略

您可以删除勒索软件策略。

查看受勒索软件保护策略保护的工作负载

在删除勒索软件保护策略之前、您可能需要查看哪些工作负载受该策略保护。

您可以从策略列表中查看工作负载、也可以在编辑特定策略时查看这些工作负载。

查看策略列表的步骤

- 1. 从BlueXP勒索软件保护菜单中、选择*保护*。
- 2. 在保护页面中,选择*管理保护策略*。

"Rans要 程序保护策略"页面将显示策略列表。

		Ransomware protectio	n strategies				
Ransomware protection strategies (4)				Q	<u>4</u>	Add	e.
Ransomware protection strategy	\$ Supplier policy	2 Backup policy	2 Detection policy	Protected workloads	:		
sps-stratage-critical	ortical-st-policy	critical-bu-policy.	rpe-policy-all	3		×	***
spi-strategy-important,	important to policy	important burpolicy	rps policy all	(0)		~	
-pi-stratagy-standard	standard-to-policy	standard-bu-policy	rps-policy-all	0		~	
725 strategy 4	standard-ss-policy-344	standard by policy-344	rps gobcy all	0		\sim	
					hill policy		

3. 在"反向器保护策略"页面上的"受保护的工作负载"列中、单击行尾的向下箭头。

删除勒索软件保护策略

您可以删除当前未与任何工作负载关联的保护策略。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。

2. 在保护页面中,选择*管理保护策略*。

3. 在管理策略页面中,为要删除的策略选择*Actions* ••• 选项。

4. 从操作菜单中,选择*Delete policy*。

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可,本文档中受版权保 护的任何部分不得以任何形式或通过任何手段(图片、电子或机械方式,包括影印、录音、录像或存储在电子检 索系统中)进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束:

本软件由 NetApp 按"原样"提供,不含任何明示或暗示担保,包括但不限于适销性以及针对特定用途的适用性的 隐含担保,特此声明不承担任何责任。在任何情况下,对于因使用本软件而以任何方式造成的任何直接性、间接 性、偶然性、特殊性、惩罚性或后果性损失(包括但不限于购买替代商品或服务;使用、数据或利润方面的损失 ;或者业务中断),无论原因如何以及基于何种责任理论,无论出于合同、严格责任或侵权行为(包括疏忽或其 他行为),NetApp 均不承担责任,即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意,否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明:政府使用、复制或公开本文档受 DFARS 252.227-7013(2014 年 2 月)和 FAR 52.227-19 (2007 年 12 月)中"技术数据权利 — 非商用"条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务(定义见 FAR 2.101)相关,属于 NetApp, Inc. 的专有信息。根据 本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质,并完全由私人出资开发。 美国政府对这些数 据的使用权具有非排他性、全球性、受限且不可撤销的许可,该许可既不可转让,也不可再许可,但仅限在与交 付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外,未经 NetApp, Inc. 事先 书面批准,不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)(2014 年 2 月)条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。