



Detect & Respond to Ransomware with Veeam ONE



Melissa Palmer

Senior Technologist, VMware Certified
Design Expert #236

Kirsten Stoner

Technical Analyst

Contents

- Part I: Detect & Respond to Ransomware with Veeam ONE Monitor 4**
 - Ransomware Monitoring OOTB5
 - Basic Backup Notifications5
 - Detecting Ransomware6
 - Suspicious Incremental Backup Size Alarm7
 - Possible Ransomware Activity Alarm8
 - Building Custom Veeam ONE Alarms9
 - Remediation Actions in Veeam ONE11
 - Alerting & Reporting12

- Part II: Detect & Respond to Ransomware with Veeam ONE Reporter 13**
 - Veeam ONE Reporter Capabilities for Ransomware Detection14
 - Backup Reporting16
 - Backup Implementation Recommendations18
 - Identifying Suspicious Activity with Veeam ONE18
 - About authors19
 - About Veeam Software20

Abstract

Veeam® ONE™, part of Veeam Availability Suite™, is a powerful tool that provides proactive alerting, monitoring and reporting in your environment. Out of the box, Veeam ONE can monitor your environment for ransomware in several different ways. Veeam ONE can take things a step further by automatically taking action when an alarm threshold is met.

Veeam ONE is extremely flexible and configurable, allowing for endless possibilities when it comes to ransomware detection.

In this paper, we take a closer look at these capabilities in Veeam ONE in two parts, based on Veeam ONE Monitor and Veeam ONE Reporter. Part I examines the capabilities for monitoring and responding to ransomware in Veeam ONE Monitor.

Part II takes a closer look at the capabilities for reporting on your environment when it comes to ransomware, including building custom reports in Veeam ONE Reporter.

Part I: Detect & Respond to Ransomware with Veeam ONE Monitor

Ransomware Monitoring OOTB

When it comes to ransomware, any defense is better than no defense at all. There are many different types of ransomware out there today, and with each passing moment each gets more sophisticated. Backup and recovery of data once it is infected by ransomware is a go-to method of beating the ransom, but if you don't know if your backups completed successfully, you could still be putting your company's data in jeopardy.











Making sure there is a recoverable backup is just one step, but it is also important to monitor the entire environment for suspicious or unusual activity. Being able to identify abnormal behavior over the network, with backup jobs or even how resources are being used, can contribute to helping stop ransomware in its tracks.

Real-time alerting about backup job success and knowing what impacts the success of backup operations can be beneficial for any business fighting ransomware or in general. Veeam ONE makes it easy to know the state of your backup jobs and their status.

Basic Backup Notifications

Basic notifications on backup jobs and whether they finished successfully or failed allows you to ensure you have data to restore from if you do experience a ransomware attack. Whether you are protecting physical, virtual, cloud or NAS devices, being notified that your backups have finished successfully and meet the company's recovery point objectives (RPOs) provides peace of mind to any IT professional.

With backups being one of the first line of defenses for ransomware alleviation, you always want to make sure backup jobs are successful, but most importantly that you can recover from them. Not only will it let you know if your backup jobs finished successfully, it will also alert you if there are machines in your environment not protected.

LATEST ALARMS			
Status	Time	Source	Name
 Warning	8/24/2020 6:49:27 PM	site1vc1.aperaturelabs.biz	Task timeout reached
 Error	8/21/2020 4:50:45 PM	site1vc1.aperaturelabs.biz	Bad vCenter Server username logon attempt
 Error	8/21/2020 4:50:25 PM	site2vc1.aperaturelabs.biz	Bad vCenter Server username logon attempt
 Warning	8/20/2020 1:25:03 PM	site2esxi-3.aperaturelabs.biz	Host synchronization failed
 Warning	8/20/2020 1:24:03 PM	HeliumRUNWIN	VM configuration file missing
 Error	8/10/2020 2:02:31 PM	site2esxi-3.aperaturelabs.biz	Connection to iSCSI storage target failure
 Warning	8/10/2020 1:10:45 PM	site2-linux-0	VM with no backup
 Warning	8/10/2020 1:10:45 PM	site2-linux-1	VM with no backup
 Warning	8/10/2020 1:10:45 PM	site2-linux-2	VM with no backup
 Warning	8/4/2020 3:11:13 AM	VeeamON-DC	VM with no backup

The above screenshot shows Veeam ONE Monitor. In this case, we have several machines that are not protected within our defined RPOs.

Alarms to notify you about a machine's protection status, along with backup job success or failure, allows you to ensure you have a backup plan ready and prepared if a ransomware attack occurs.

Veeam ONE can notify on the current state of your backup server, data protection operations and the connectivity between enterprise manager, proxies, repositories and more. When data is compromised, being able to get the data back by restoring from a backup is an essential first response plan for any business. Monitoring backup job success, visibility into the data center and the ability to quickly respond to any issue affecting backups is just one way you can ensure that you are being protected. Veeam ONE even has the intelligence to look at the data restore points and address if data is experiencing abnormal changes or activity.

Detecting Ransomware

One way to detect ransomware and prevent spread is through monitoring your environment for suspicious activity.

Veeam ONE comes with predefined alarms that check certain counters for suspicious activity. Monitoring for abnormal activity can help remediate issues or potentially remove machines on the network before ransomware encrypts more data.

Veeam ONE comes with two out-of-the box alarms that can identify abnormal levels of resource usage and high change rate on VMs. These alarms, Suspicious Incremental Backup Size and Potential Ransomware Activity, monitor your machines in real time and are triggered when their specific resource thresholds are met.

With each alarm in Veeam ONE, there are adjustable baseline counters that you can change based on the machine it's assigned to or all the machines in the environment.

Suspicious Incremental Backup Size Alarm

The Suspicious Incremental Backup Size alarm analyzes the last three backup incremental jobs and identifies if the incremental has grown over 150%. This identifies if the newly created restore point size is significantly different from the previously created ones.

If the incremental backup run is significantly different in size, this could indicate the presence of malware on the machine, which would in turn require further investigation.

The screenshot shows the 'Alarm Settings' dialog box in Veeam ONE, specifically the 'Rules' tab. It displays two configured rules for 'Incremental backup size'. Both rules are enabled and set to trigger when the backup size is 'Above' a certain percentage. The first rule is for 'Backup' jobs, with a warning threshold at 150.0% and an error threshold at 200.0%. The second rule is for 'Agent Backup Job', also with a warning at 150.0% and an error at 200.0%. The analysis depth is set to 3. The dialog includes tabs for 'General', 'Rules', 'Assignment', 'Notifications', 'Actions', 'Suppress', and 'Knowledge base'. On the right side, there are buttons for 'Add...', 'Move up', 'Move down', 'Link...', 'Unlink', 'Remove', and 'Defaults'. At the bottom, there are 'Save' and 'Cancel' buttons. A note at the bottom states: 'By default rules work with the OR logic.'

By default, the alarm will trigger when the incremental backup size has grown by 150% with a warning and 200% with an error. These counters are adjustable, so you can change them to notify you based on the percentage change.

This alarm doesn't just look at VM backup jobs, but also any computers running the Veeam Agent. This alarm is assigned based on backup infrastructure, so if you have multiple backup servers added in Veeam ONE, you can have this alarm set for a specific backup server or all. Additional options that can be set for any alarm are remediation actions, suppression settings and notifications.

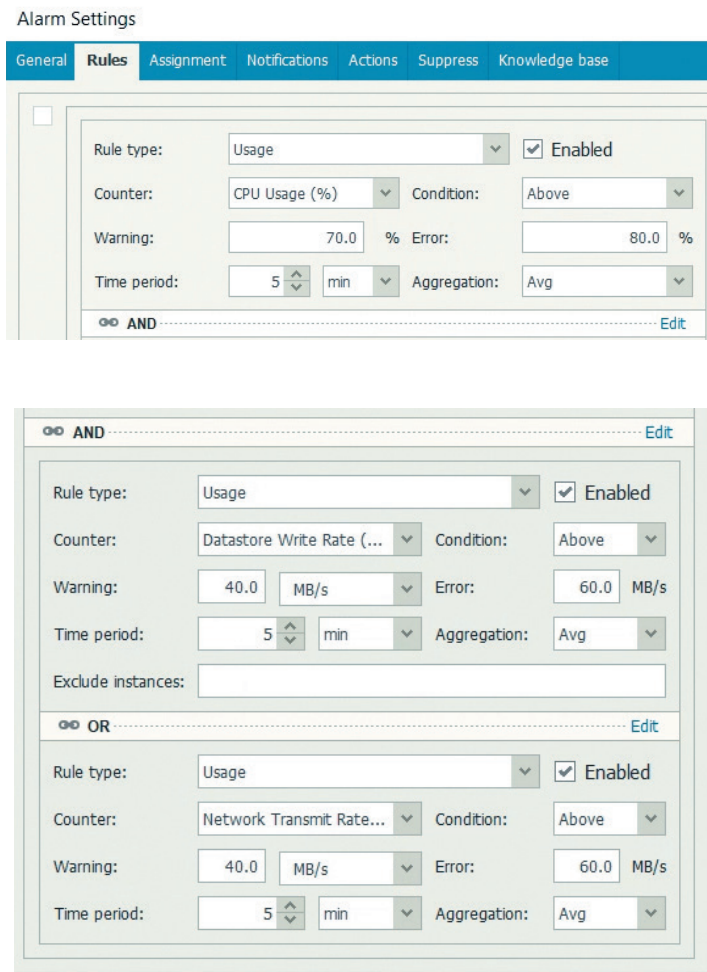
If you would like to customize an alarm's parameters, it is always a good idea to make a copy of the alarm first. You can have multiple copies of the alarm in your environment configured with different parameters, and they can be assigned to different Veeam Backup & Replication™ servers as applicable.

Possible Ransomware Activity Alarm

Other resources Veeam ONE can monitor through its alarms are CPU usage, datastore write rate and network transmit rate. By monitoring the usage of these activities in the machine, the Possible Ransomware Activity alarm can identify if this is suspicious activity for the machine to be experiencing.

These higher-than-normal writes on disk or CPU utilization could be a sign that ransomware infected the machine. The goal of the alarm is to pinpoint the machine that is potentially infected before it can propagate to other systems.

The default parameters examined for the alarm are as follows:



Once again, these parameters can be customized.

Because these are applied at the Virtual Infrastructure level, you can create copies of this alarm and apply them at the VM or VM group level via business view rules.

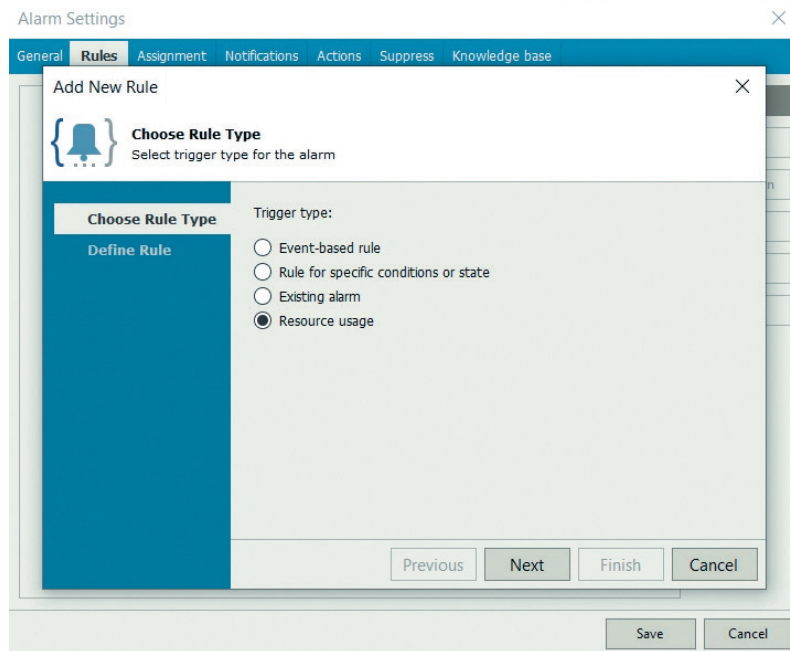
For example, if you are confident in a certain application's performance profile, you can create a copy of the Possible Ransomware Activity alarm specifically with those parameters.

Additional parameters can also be added to the alarm as you deem fit by your requirements.

Building Custom Veeam ONE Alarms

Beyond customizing the already-provided alarms for ransomware detection, completely custom alarms can be created in Veeam ONE. Existing alarms can also be copied and modified.

Alarms in Veeam ONE are based on rules, which can have many definitions and parameters. With Veeam ONE alarm rules, you can monitor most aspects of your virtual machines, and you can have multiple rules per alarm.



When it comes to creating custom alarms to monitor your environment for ransomware, there are many possibilities.

Resource usage is always an interesting area to examine, since in many cases we know how our virtual machines are expected to behave by looking at their historical performance data in Veeam ONE.

Some examples of resources you can monitor for your virtual machines are:

- CPU usage
- Virtual disk write I/O
- Guest free disk space
- Memory usage
- Network transmit rate
- And many others

You can also create custom alarms to monitor your vSphere or Hyper-V hosts.

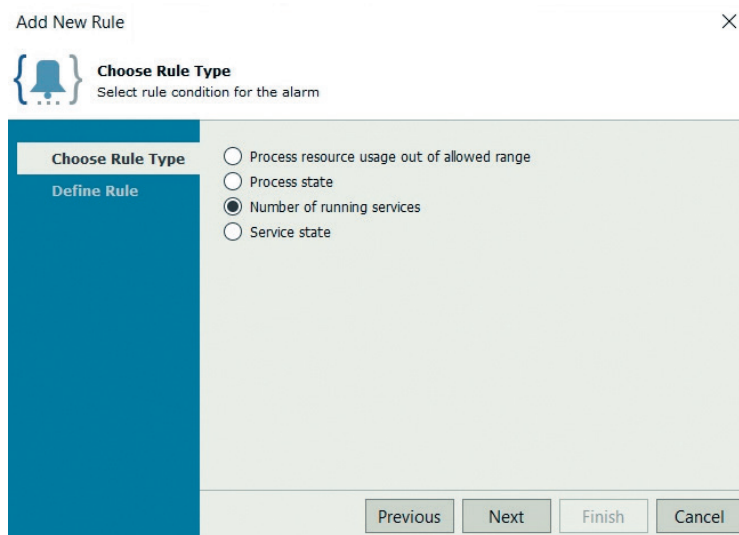
Note: Please see the Complete Alarm Rules for VMware vSphere https://helpcenter.veeam.com/docs/one/alarms/vsphere_alarm_rules.html?ver=100 and the Complete Alarm Rules for Hyper-V https://helpcenter.veeam.com/docs/one/alarms/hyperv_alarm_rules.html?ver=100 to see the complete capabilities of what Veeam ONE can monitor.

Let's take a look at an interesting use case for one of these Rule Trigger Types.

Monitoring Number of Running Services

An alarm can be created to monitor the number of running services on your virtual machine. In this case, you would use the **Rule for specific conditions or state**, and select **Processes and services**.

There are a number of rules that can be leveraged when it comes to processes and services:



One interesting thing to monitor is the number of running services. In the event a piece of malware starts a new service, the alarm would then be triggered in Veeam ONE.

At this point, beyond generating an alert, Veeam ONE could also take action via a remediation action.

Remediation Actions in Veeam ONE

Remediation actions are a method to take action after an alarm has been triggered in Veeam ONE. There are a number of alarms that have pre-configured remediation actions out of the box.

One of the most popular Veeam ONE alarm and remediation action combinations is the VM with no backups alarm. When this alarm is triggered, a number of actions can be configured to execute, such as:

- Add VM to backup job
- Add VM to backup job and run
- Run parent backup job
- Start quick backup
- Start VeeamZIP

These actions can execute automatically, or by approval if a remediation action is set to by approval. It will need to be approved in Veeam ONE Monitor before it executes.

NOTE: For a complete list of pre-defined remediation actions in Veeam ONE, please see:

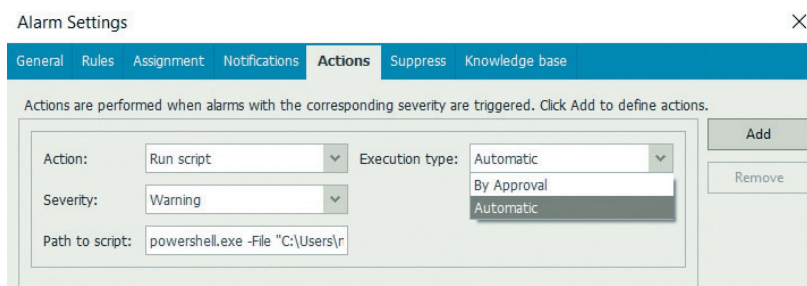
https://helpcenter.veeam.com/docs/one/alarms/appendix_remediation.html?ver=100

Creating Custom Remediation Actions

Creating a custom remediation action is simple.

First, a script that can be executed by Windows must be created to accomplish the action.

After the script has been created, the Actions tab should be configured in the Veeam ONE alarm that will serve as the trigger:



First, depending on how you configured your alarm, decide if you would like to run your remediation action when the information, warning, or error thresholds of the alarm are met. You can also have multiple remediation actions in an alarm to act on each threshold, or to simply perform multiple tasks.

Simply enter the path to the script you would like to execute, and then decide if you would like to execute Automatically or By Approval.

Veeam ONE remediation actions are flexible and allow Veeam ONE to execute virtually any action that meets the requirements within your environment.

For example, you may choose to create remediation actions based on the out-of-the-box ransomware alarms in your environment, or ransomware alarms you created or customized on your own.

Let's take a look at two possible ways you can respond to ransomware alarms to get a few ideas.

The first example would be to disconnect your VM from the network if a ransomware alarm is triggered. Since this will impact production, you may want to set this to By Approval, and ensure the alarm is also sending alerts to your operations team. Your team will then be quickly alerted, and can determine if they want to go ahead and disconnect the network card for further investigation.

Another example would be to run a preconfigured SureBackup® job with Virus Scan enabled. This would be non-invasive to your production environment, so you may set a remediation action to automatic, and be sure your operations team is promptly alerted.

NOTE: For more on configuring a custom remediation action, see the Veeam ONE documentation

https://helpcenter.veeam.com/docs/one/alarms/alarm_actions.html?ver=100

Alerting & Reporting

After alarms have been configured, there are two more important things to think about when it comes to using Veeam ONE to help detect ransomware in your environment: Alerting when Veeam ONE alarms are triggered and generating helpful reports in Veeam ONE Reporter.

Alerting on Ransomware Activity in Veeam ONE Monitor

Beyond an alarm being visible in Veeam ONE Monitor, there are a number of notification actions that can be taken when an alarm is triggered.

- Send email to a default group
- Send email notification
- Send SNMP trap
- Run script

Configuring the appropriate notifications in your environment ensures you will always be promptly alerted to suspicious activity in your environment. Multiple notification options can also be configured.

NOTE: For more information on how to configure Veeam ONE alarm notifications, please see the Veeam ONE documentation.

https://helpcenter.veeam.com/docs/one/alarms/alarm_notifications.html?ver=100

Part II: Detect & Respond to Ransomware with Veeam ONE Reporter

Veeam ONE Reporter Capabilities for Ransomware Detection

There are several reports in Veeam ONE Reporter that can assist with monitoring your environment from a ransomware perspective.

First and foremost is the VM Change Rate History report in the Veeam Backup Monitoring category.

When malware infects a machine, it starts encrypting and changing the data, making it inaccessible. The VM Change Rate History report wasn't initially intended for detecting ransomware, but since it looks at how the machine is changing, specifically the amount of changed data, it can help identify if there is abnormal activities occurring in the machine. For a better understanding of this report, it analyzes the incremental run of the backup job. Since Veeam Backup & Replication uses Change Block Tracking (CBT) technology, it analyzes those blocks of data that have changed and then backs up only the changes of that data. If malware is installed and changing data, this counter could be higher than expected in most cases.

This report easily identifies the top VMs based on their change rate and drills down to specific backup jobs, the VMs included and the average change rate of those VMs.



VM Change Rate History

Description

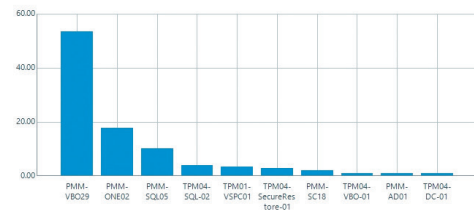
This report shows jobs whose backup files and replica VMs grow fast and may quickly consume space on the target repository or datastore.

Report Parameters

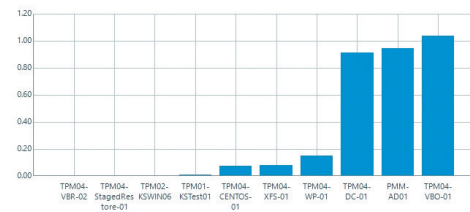
Scope: Virtual Infrastructure
Interval: Current week (9/14/2020 - 9/20/2020)
Job type: All jobs
Job Exclusion list: -

Summary

VMs with Largest Change Rate (GB)



VMs with Least Change Rate (GB)



Details

Job Name	VM Name	Average VM Change Rate Per Day (GB)	Total Incremental Changes (GB)	Total Active Full Backups Data (GB)	Actual Increments File Size (GB)	Actual Full Backup File Size (GB)	Total Backup File Size (GB)	Actual N. of Increments	Actual N. of Full Backups
10.0.40.10\Backup Job 14	1	0.25	0.74	0.00	2.31	2.77	5.07	5	2
10.0.40.10\Cloudian Demo - Image Based Backup - Immutable	3	0.26	0.77	0.00	9.02	19.87	28.89	15	5
10.0.40.10\Snapshot-less Orchestrated Snapshot - Multi	2	0.00	0.00	0.00	0.00	0.00	0.00	0	21
10.0.40.10\Snapshot-less Orchestrated Snapshot - SQL	1	0.00	0.00	0.00	0.00	0.00	0.00	0	23
10.0.40.10\VMware Backup - Application Stack	5	1.63	4.90	0.00	13.71	49.68	63.38	10	2
10.0.40.10\VMware Backup - Domain Controllers	1	0.30	0.91	0.00	14.60	41.24	55.83	15	3
10.0.40.10\VMware Backup - Local DAS	1	0.25	0.74	0.00	5.72	4.97	10.68	15	3
10.0.40.10\VMware Backup - VBC365	1	0.35	1.04	0.00	12.13	47.04	59.17	16	3
10.0.40.10\VMware Backup - Web Server	1	0.01	0.04	0.00	0.59	2.32	2.92	16	3
TPM01-KS100\Example 01 - VMware VMs	2	1.11	3.34	0.00	5.83	319.41	325.24	3	2
	TPM01-KSTest01	0.00	0.00	0.00					
	TPM01-VSPC01	1.11	3.34	0.00					
TPM01-KS100\Example 02 - Azure	1	0.64	1.91	0.00	2.11	25.87	27.98	12	3
	PMM-SC13	0.64	1.91	0.00					
TPM01-KS100\Example 03 - PMM SQL	2	8.14	23.41	0.00	138.92	296.20	435.13	12	4
	PMM-ONE02	6.25	17.72	0.00					
	PMM-SQL05	1.90	5.69	0.00					
TPM01-KS100\Example 07 - Cloud Connect	2	0.00	0.00	0.00	6.97	43.17	50.14	7	2
TPM01-KS100\Example 08 - VMR	3	19.61	58.82	0.00	49.15	230.11	279.26	13	5
	PMM-AD01	0.32	0.95	0.00					
	PMM-SQL05	1.52	4.55	0.00					
	PMM-VBC09	17.78	53.33	0.00					

Report created: Wednesday, September 16, 2020 12:35:46 PM (UTC-08:00) Pacific Time (US & Canada)

Page: 2 of 2

The report above identifies VMs with the largest and least amount of change rate based on backup job runs. The change rates in this report are based on changes occurring on the VM disks. This can help you identify VM files that are increasingly growing.

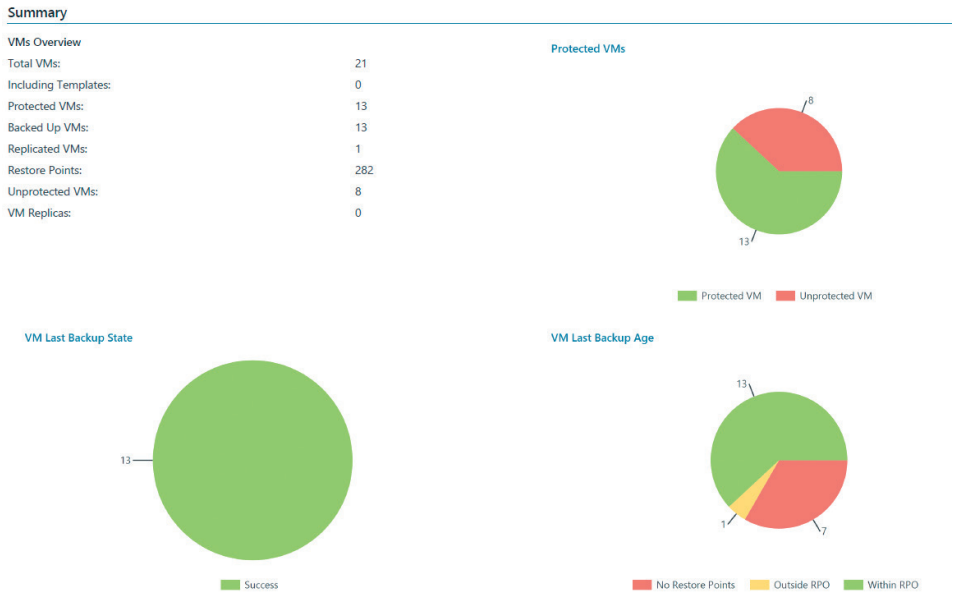
Veeam ONE contains many different reports that not only show how your machines are changing from a production viewpoint with how many resources its consuming, but also how the backup files are growing. Since ransomware changes the files on the machine, running multiple reports to analyze the environment can contribute to pinpointing abnormal behavior.

The Veeam Backup Files Growth report can help with capacity planning for backup repositories, but it can also allow you to have visibility on how much your backup files are growing. The report can identify backup files that grow too fast, so you can reconfigure backup jobs as you see fit. However, since it takes a look at how backup files are growing, it's important to be aware of how the data is changing and growing to identify what could be considered abnormal.

Similar to alarms, reports can be set up to be delivered to your inbox, so you can check these reports daily, tracking VM change rate and growth.

Backup Reporting

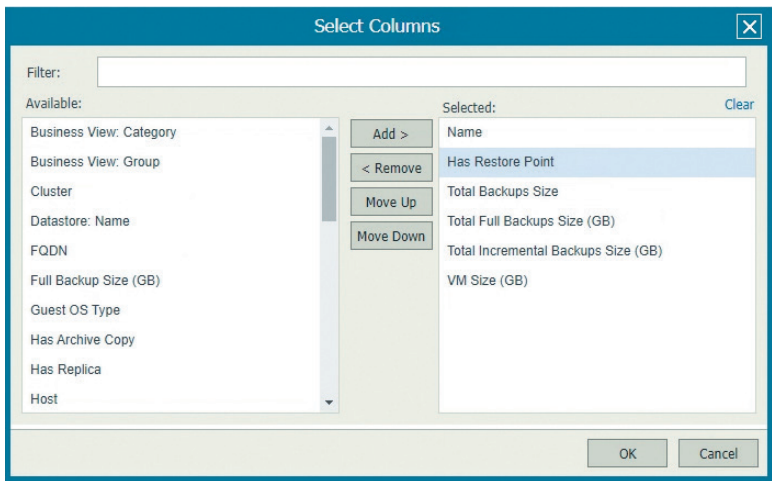
We've discussed how one of the ways to remain resilient in the fight against ransomware is to ensure your data is properly protected, so if you were to experience an attack, you can restore from a backup. The protected VMs report helps identify machines that are meeting recovery point objectives (RPOs) with a valid restore point within this specified time period. Along with identifying those machines that are protected, it shows which machines are not protected. This report is available for any workload you are using Veeam to protect: physical, cloud or virtual machines.



Right from the front page of the report, you can see how many of your machines are protected or unprotected. As you flip through the rest of the report, you can see the names of the VMs and the date of the last successful job run.

The reporter allows you to build reports based on different parameters, so if the predefined reports included don't fit your needs, you can create one. Custom reports allow you to define your own configuration parameters, performance metrics and filters.

The Backup Infrastructure Custom data report enables you to base the report on your backup objects such as backup servers, backup jobs, VMs and computers. For example, you want a report that tells you if your virtual machine has a valid restore point (to make sure you can recover), you want to see the size of the backup file, how big its increments are, and lastly, you want to make sure the VM isn't growing too large. This is easily configurable in the custom reports section of Veeam ONE Reporter.



There are several different properties you can base the report on. I chose these properties because I want to make sure I have a valid restore point and because I'm keeping an eye out on how big my backups are and how big my VMs are becoming.



Backup Infrastructure Custom Data

Description

This report allows to define your own parameters and filters to get custom backup information. The report should be used if maximum flexibility is required.

Report Parameters

Scope: tpm01-1st100
 Object Type: Virtual Machine
 Columns: Name, Has Restore Point, VM Size (GB), Total Full Backups Size (GB), Total Incremental Backups Size (GB), Total Backups Size
 Custom Filter:

Details

Name	Has Restore Point	Total Backups Size	Total Full Backups Size (GB)	Total Incremental Backups Size (GB)	VM Size (GB)
PMM-ONE02	True	304.16	204.63	99.53	262.39
PMM-SQL05	True	262.97	183.83	79.13	99.38
PMM-ADS1	True	38.63	31.17	7.46	23.58
TPM02-KSWIN06	True	50.14	43.17	6.97	84.62
PMM-VOVBR30	True	37.93	37.93	0.00	58.15
PMM-10P19	True	7.97	7.92	0.05	0
PMM-VBG09	True	108.63	106.68	1.95	75.29
VBR-PRX-LB7-2	True	1.15	1.15	0.00	17.91
PMM-VBFRFE50	True	17.41	17.41	0.00	69.25
TPM01-PROXY	True	9.86	9.86	0.00	62.39
TPM01-VSPC01	True	288.42	262.64	5.78	262.6
PMM-ADS1	True	12.05	12.05	0.00	130.98
PMM-SC18	True	70.15	61.12	9.03	24.09
TPM01-KSTest01	True	56.82	56.77	0.05	260.87
TPM01-CE01	True	27.05	27.05	0.00	108.89
PMM-VOVAL33	True	2.24	2.24	0.00	8.26

The ability to create custom reports provides a view of key aspects of my environment that might not be shown in a pre-defined report. Once you save the report, you can set it up to be emailed to your inbox.

Report customization isn't limited to only backup objects. If you have your vCenter server added into Veeam ONE, you can create reports based on your virtual environment as well. The VMware custom performance report can show visibility into performance issues in your environment. You can monitor specific CPU, memory, network and disk metrics to analyze the performance of vSphere hosts, datastores and VMs.

Backup Implementation Recommendations

Be sure to see the latest advice for implementing Veeam Backup & Replication to be resilient against ransomware: <https://www.veeam.com/wp-beat-ransomware-education-implementation-remediation.html#wpty>

Identifying Suspicious Activity with Veeam ONE

No one is immune to ransomware, with home users, businesses and public agencies all being a target. The best defense is to have a strategy outlined for when it happens and not fall victim to only being able to respond after it happens. With the virus encrypting files and different data types, there is potential for it to spread through computers, network shares or exploits.

Backing up your data, is only one way you can recover from an incident, but when it comes to email phishing or other means of ransomware encryption and entry into the environment, security awareness training and ensuring software is being updated to reflect the current landscape can be beneficial. Being resilient and having visibility into your data center through different monitoring and reporting tools can help stop the spread and contain the virus so it doesn't cost more downtime or data loss.

When it comes to ransomware, having a strategy to prevent but also recover from a malicious attack should be an important part of any business strategy. Veeam ONE provides visibility into the virtual environment, providing alerts on resources usage in real-time. With two out-of-the-box alarms plus the ability to create custom alarms based on tasks or events, performance usage and in-guest processes and services, Veeam ONE is a great tool to start using to prevent and combat the threat.

Real-time alerting and reporting capabilities that allow you to keep an eye on activity that is normal as well as suspicious and unusual can keep any business resilient. At this stage of ransomware intelligence, it's not a matter of if, but when, with monitoring tools like Veeam ONE providing an extra level of visibility to keep your data safe.

About authors



Melissa Palmer is Senior Technologist on the Product Strategy team at Veeam and a VMware Certified Design Expert (VCDX-236). Melissa has been focused on the full infrastructure stack in her career, and started out as an VMware engineer for a number of enterprise environments. You can find Melissa on twitter @vMiss33 or at her blog <https://vMiss.net>.



Kirsten Stoner is a Technical Analyst on the Product Strategy team at Veeam Software. Kirsten has specialization focused on technical community interaction in forums and events online and around the world. Kirsten holds the Veeam Certified Engineer (VMCE) credential and specializes in Veeam's backup and management products. Kirsten has an additional specialization in Veeam's popular Community Edition, a free offering to the IT community.

About Veeam Software

Veeam® is the leader in Backup solutions that deliver Cloud Data Management™. Veeam provides a single platform for modernizing backup, accelerating hybrid cloud and securing your data. With 365,000+ customers worldwide, including 81% of the Fortune 500 and 66% of the Global 2,000, Veeam customer-satisfaction scores are the highest in the industry at 3.5x the average. Veeam's global ecosystem includes 70,000+ partners, including HPE, NetApp, Cisco and Lenovo as exclusive resellers. Headquartered in Baar, Switzerland, Veeam has offices in more than 30 countries. To learn more, visit <https://www.veeam.com> or follow Veeam on Twitter @veeam

veeam

Cloud Data

Backup
for what's next

5 Stages of Cloud Data Management —
start your journey today!

Learn more: [veeam.com](https://www.veeam.com)