Runecast

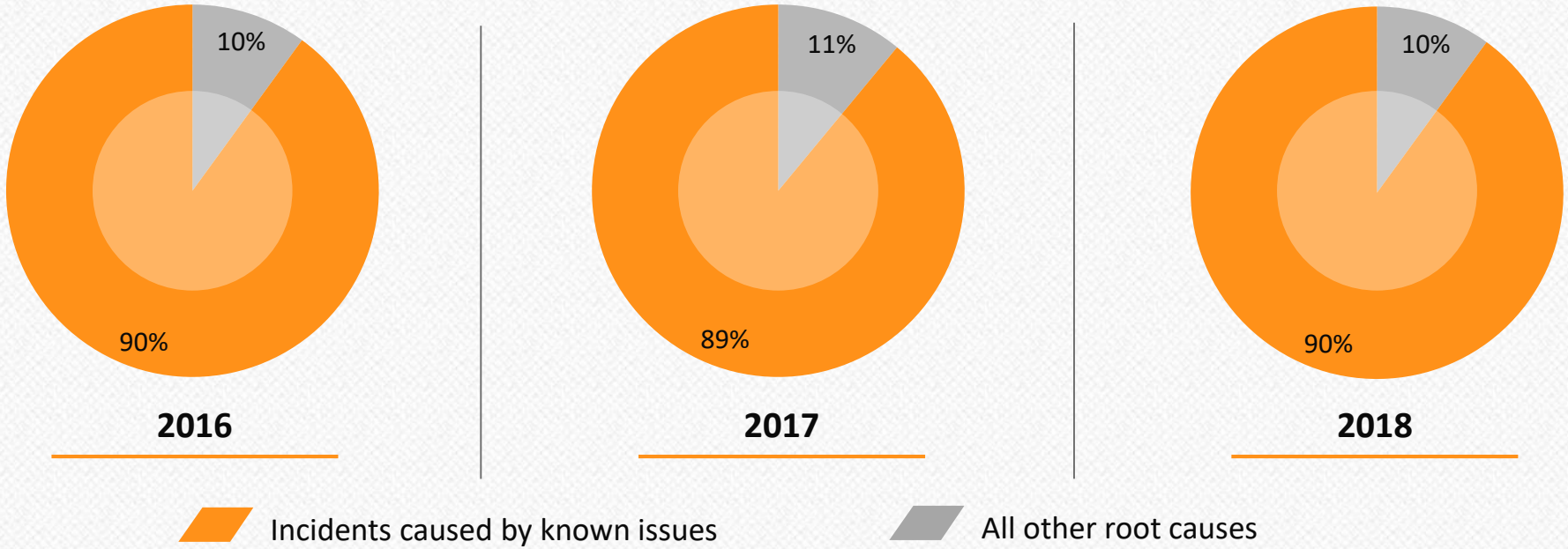
Less troubleshooting. More innovating.

PRIANTO

Prianto Hungary and CEE value-added distributor
Prianto GmbH
Kőér u. 2/A, 1103 Budapest, Hungary

Tel: +36 70 418 7177
Email: oliver.urzica@prianto.com
www.prianto.hu

90% of VMware SDDC problems caused by known issues



- Remediation usually takes hours of Googling, reading and filtering through documentation in:
  - **VMware Knowledge Base**
  - **Best Practices**
  - **Security Hardening Guides**
- This great wealth of knowledge is only being leveraged reactively after issues happen.

Why not apply these vast resources proactively?

Typical problems in a VMware SDDC

- **Knowledge Base (KB)**
  - 30,000+ known issues documented in KB – constantly updated and expanding.
  - Manually checking for them all is not humanly feasible.
  - Most environments contain many latent issues that Admins are unaware of.
  - When latent issues surface they cause system degradation, outages and/or breaches.

- **Best Practices**
  - Best practices often overlooked – hard to monitor.

- **Security Compliance**
  - Achieving security compliance manually places a huge drain on resources.

- **Logs**
  - The huge volume of logs makes it very difficult to identify any problems they expose.

All that info but your environment is a minefield

Runecast Analyzer solves these problems

- Runecast **proactively** identifies the **causes** of issues **before** they occur, does all the root cause analysis work for you and provides the solution to remediate.
- Proactively scans your **vSphere, vSAN, NSX and Horizon** environment against:
  - VMware Knowledge Base.
  - VMware Best Practices.
  - VMware Security Hardening Guides
  - Security standards such as DISA-STIG 6, PCI-DSS and HIPAA
- **Configuration Analysis** – analyses all configurations in your environment and correlates them against KBs, BPs and Security Guides and other standards.
- **Log Analysis** – correlates logs in real-time against KBs and sniffs for problematic logs.
- Automates continuous security compliance checks.

Proactive management with 100% transparency on latent issues

Runecast Analyzer

- **Detects**
  - Identifies all known KB issues, BP violations, security weaknesses and misconfigurations.
  - Real-time logs are correlated **against** KBs to **easily identify** root causes of operational issues.
- **Informs**
  - Identified issues are **grouped** by level of severity.
  - Info to remedy each issue is provided with just one click.
  - Automated email alerts / reports.
- **Secures**
  - Automates continuous security compliance against Hardening Guides, KBs & DISA-STIG.
- **Optimizes**
  - Ensures optimal configuration for trouble-free operation.

Minimize risks – Reduce outages - Enhance Security

A few key points

- Deploys as an OVA file and runs on-premises as a lightweight virtual appliance
- Deploy and configure in 5 to 10 minutes – just a few clicks
- Supports multiple vCentres, vSAN, NSX-V and Horizon
- Handles multiple vSphere versions (5.x - 6.x) and combinations
- Extremely fast with 100's of thousands of checks in 1 – 2 minutes
- Never uploads data from your datacentre & supports online or offline updates
- Extremely intuitive and easy-to-use – no learning curve.
- Full REST API for integration with other tools and management solutions
- vSphere Web Client plugin supports Flex/Flash and HTML5 versions (i.e. versions 6.x & up)
- vRealize Orchestrator plugin for auto-remediation workflows
- AWS certified for VMware Cloud on AWS

Secure - Lightweight – Fast - Intuitive

How does it fit with your existing tools?

- Complements functionality of tools like vROPS, Log Insight, Veeam One and Turbonomics.
- Other tools focus primarily on capacity and performance management - they **reactively** identify **symptoms** of issues **after** they occur and then leave you to search for a cause / solution.
- Runecast **proactively** identifies the **causes** of issues **before** they occur, does the root cause analysis work for you and provides the solution in just one click.
- Full REST API for integration with other tools and management solutions.
- vCenter Web Client plugin supports both the Flex/Flash and HTML5 versions.
- vRO plugin for automation workflows.

Supplements functionality of your existing tool mix

Business benefits

Save time

Less troubleshooting and health-checking. More time for innovating.

Reduce outages

Discover and remediate hidden issues before they cause outages.

Improve Security

Continuous security compliance, security KBs, secure architecture.

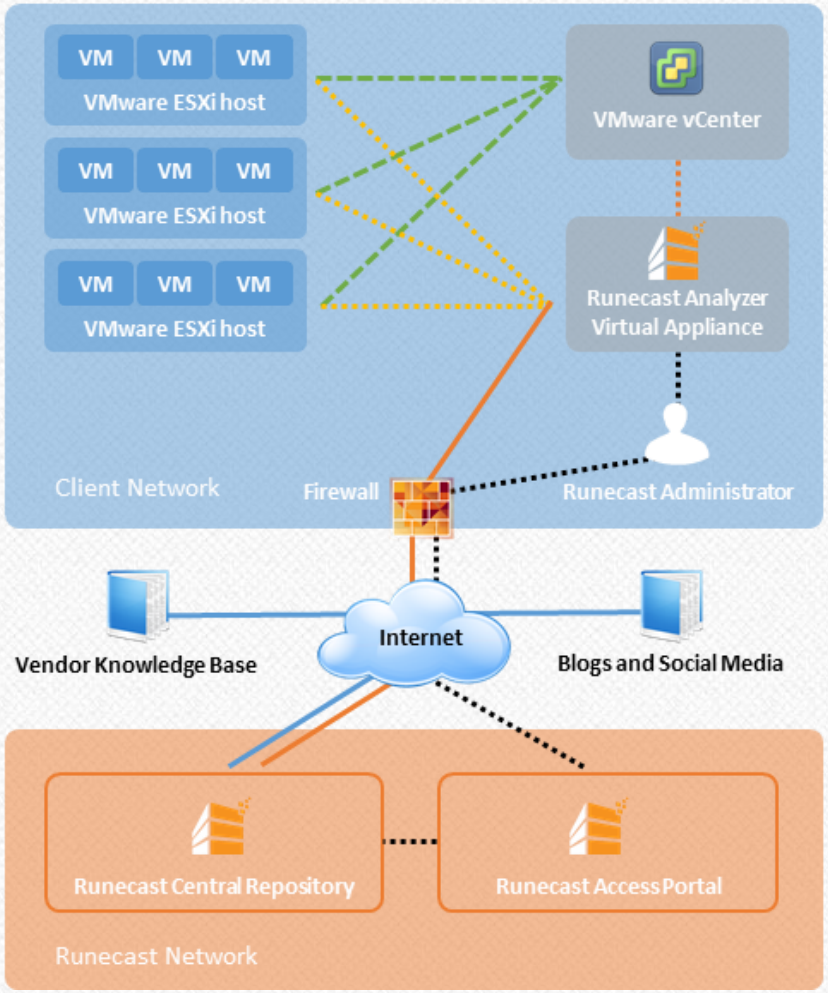
Minimize risk with continuous compliance

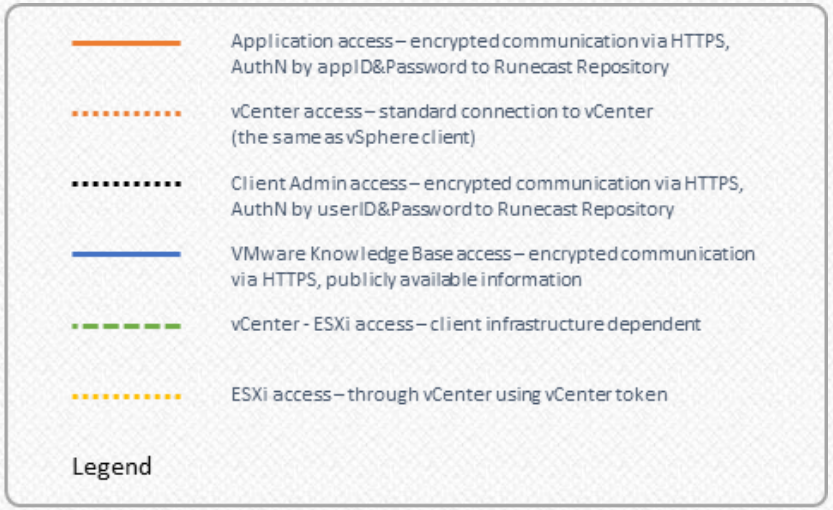
Your environment now follows industry best practices and is configured in the most optimal way.

Reduce costs

Prevent outages, save time and avoid audit penalties.

Secure Architecture





Testimonials

"Runecast Analyzer gives me peace of mind knowing the servers are better optimized, configured, patched and secured, which mitigates downtime and saves a lot of man hours."

Marc Crawford, Senior System Engineer, NJVC

"I highly recommend this solution as a 'must have' for any VMware vSphere environment."

Stephen Parker, System Engineer, BYU Idaho

"Runecast Analyzer increases the stability and performance of our environment…We have a mission next year that will encompass a greenhouse in space so Runecast Analyzer is actually going to help us to grow food in space!"

Michael Szczuka, Senior Engineer, German Aerospace Center (DLR)

"Runecast Analyzer is the tool we always wanted from VMware."

Nicolas Maeder, Senior System Engineer, UMB AG

Main Dashboard

Runecast

CONTEXT

All vCenters

MAIN MENU

- Dashboard
- Inventory view
- All issues view

CONFIGURATION ANALYSIS

- Config KBs discovered
- Best practices
- Security hardening

LOG ANALYSIS

Analyze now

Main Dashboard

Configuration issues by severity

Critical 265

Major 154

Medium 154

Low 98

Log issues

2

Security compliance

DISA STIG 6

54%

Configuration issues

200

Best practice adoption

89%

Configuration issues by layer

Management (34)

23 11

Issues history

Day Week

600

400

Issues View

All Issues View

Export

vCenters | Severity | Source | Applies to | Affects | Products

Search

October 1, 2018 - November 28, 2018

Issues count history (per scan)

500
400
300
200
100
0
Oct 24, 2018
Nov 4, 2018
Nov 15, 2018
Nov 26, 2018

Current issues

300
200
100
0

Critical
Major
Medium
Low

Results: Cur Compare with previous result

Severity	Source	Applies	Affects	Products	Objects	Title
Critical			Availability	vSphere	1	ports the error: tcp_input (2136430)
Critical		Compute	Availability	vSphere	2	ning Vmxnet3VMKDevRxWithLock (2144968)
Critical	KB	Compute	Availability	vSphere	7	Virtualization Technology Erratum (2147325)
Critical	KB	vCenter	Security	vSphere	1	Center Server 6.0 (2149434)
Critical	KB	Compute	Availability	vSphere	1	ximum" in the ESXi 6.0 host (2145654)
Critical	KB	Compute	Availability	vSphere	1	PSOD karound for Apache Struts -qlgc_cn" in ESXi host (2145793)
Critical	KB	Compute	Availability	vSphere	1	ESXi host fails with the error: PANIC bora/vmkernel/main/dlmalloc.c:xxxx - Corruption in dlmalloc (2147888)

ESXi host fails with a purple diagnosti
ESXi 6.0 Update 2 host fails with a PS
ESXi host fails with a diagnostic scre

Historical Changes

Runecast

CONTEXT

All vCenters

MAIN MENU

Dashboard

Inventory View

All Issues View

CONFIGURATION ANALYSIS

Config KBs Discovered

Best Practices

Security Hardening

LOG ANALYSIS

Log KBs Discovered

Log Inspector

Analyze now

All Issues View

Export

vCenters | Severity | Source

Search

November 21, 2018 - November 27, 20

Issues count history (per scan)

500 400 300 200 100 0

Nov 21, 2018

Nov 27, 2018

Current issues

Critical

Major

Medium

Low

Results: Nov 26, 2018 12:19 P

Severity | Source

Critical KB

Critical KB

Critical KB

Critical KB

Critical KB

Critical KB Compute Availability vSphere 1 ESXi host fails with the error: PANIC bora/vmkernel/main/dlmalloc.c:xxxx - Corruption in dlmalloc (2147888)

Critical KB Compute Availability vSphere 1 ESXi host or virtual machine hangs after approximately 85 days (2147739)

Critical KB vCenter Security vSphere 10 Hypervisor-Assisted Guest Mitigation for Branch Target Injection (52085)

th a purple diagnostic screen and reports the error: tcp_input (2136430)

2 host fails with a PSOD error mentioning Vmxnet3VMKDevRxWithLock (2144968)

th a diagnostic screen due to an Intel Virtualization Technology Erratum (2147325)

Apache Struts CVE-2017-5638 for vCenter Server 6.0 (2149434)

KAPI-char-metadata heap at maximum" in the ESXi 6.0 host (2145654)

Exception 14 in world sfcb-qlgc_cn" in ESXi host (2145793)

Results Comparison

‹ Previous

Nov 26, 2018 11:51 AM > Nov 26, 2018 12:19 PM

Next ›

Summary

New issu total vCenters scanned

91 2

Change Log (253)

qlnativefc driver cause interm onnection (2134218)

Resolved Issue detail

Disable SSH unless needed for diag bleshooting

Partially resolved 3 objects Iss

exity: ESXi.set-

Establish a password policy for password-policies (8.2.4)

New 1 objects Issue rd complexity: ESXi.set-

New 1 objects Issue detail

For an ESXi account, a new passwords set is not allowed to resemble the previously four set passwords. (8.2.5)

New 1 objects Issue detail

VMware Security Advisory: VMSA-2018-0017.4 (VMware Tools update addresses an out-of-bounds read vulnerability)

Activity

deneb-vc60.outer.space (1)

deneb-esxi60-04.outer.space resolved

Close

Issue Details

Runecast

CONTEXT

All vCenters

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices
- Security Hardening

LOG ANALYSIS

- Log KBs Discovered
- Log Inspector

Analyze now

Config KBs Discovered

Export

Severity | Applies to | Affects | Products | Search

Severity	Applies to	Affects	Products	Objects	Title
Critical	Compute	Availability	vSphere	2	ESXi 6.0 Update 2 host fails with a PSOD error mentioning Vmxnet3VMKDevRxWithLock (2144968)
Critical	Compute	Availability	vSphere	3	ESXi 6.x vSAN host experiences a purple diagnostic screen at bora/modules/vmkernel/lsomcommon/ssdlog/ssdopslog.c:199 (2146345)
Critical	Compute	Availability	vSphere	3	ESXi IO connectivity issues or PSOD with VT-d interrupt remapper disabled (2149592)
Critical	Compute	Availability	vSphere	3	ESXi host fails with PSOD after upgrading to 6.5 (2151749)
Critical	Compute	Availability	vSphere	7	ESXi host fails with a diagnostic screen due to an Intel Virtualization Technology Erratum (2147325)
Critical	Compute	Availability	vSphere	1	ESXi host fails with a purple diagnostic screen and reports the error: tcp_input (2136430)
Critical	Compute	Availability	vSphere	4	ESXi host fails with purple screen error: "NOT_IMPLEMENTED bora/vmkernel/filesystems/devfs/devfs.c:2655" (2150280)
Critical	Compute	Availability	vSphere	1	ESXi host fails with the error: PANIC bora/vmkernel/main/dlmalloc.c:xxxx - Corruption in dlmalloc (2147888)

Details | Findings | Note

Ignore

Affected objects

antares-vc65.outer.space

antares-esxi65-1.outer.space

antares-esxi65-2.outer.space

antares-esxi65-3.outer.space

(3)

Automatic checks

Object	Finding description	Finding value
antares-esxi65-1.outer.space	Host version	VMware ESXi 6.5.0
antares-esxi65-1.outer.space	Host build number	5310538
antares-esxi65-1.outer.space	Host has 10 Gigabit Ethernet adapter	vmnic0
antares-esxi65-1.outer.space	Host has 10 Gigabit Ethernet adapter	vmnic1
antares-esxi65-1.outer.space	Host NetQueue status	Enabled

Security Hardening

Runecast

CONTEXT

All vCenters

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices
- Security Hardening
  - VMware Guidelines
  - DISA STIG
  - PCI DSS
  - HIPAA

LOG ANALYSIS

- Log KBs Discovered
- Log Inspector

Analyze now

Major	Compute	vSphere	3	Enable lockdown mode to restrict remote access: enable-lockdown-mode	Fail
Major	Network	NSX-V	1	Ensure that NTP	Fail
Major	Network	NSX-V	1	Ensure the Forged Transmits policy is set to ...word	Fail
Major	Network	vSphere	3	Ensure that the MAC Address Change policy is set to reject ...transmit	Fail
Major	Network	vSphere	3	Establish a password policy for password complexity: ESXi.... ...anges	Fail
Major	Compute	vSphere	3	...icies	Fail
Major	Network	NSX-V	1	Follow VMware Security Advisories and apply patches: keep-...	Fail
Major	Compute	vSphere	3	Keep ESXi system properly patched: ESXi.apply-patches	Fail

Details | Findings | Note | Ignore

Affected objects

- antares-vc65.outer.space
  - **antares-esxi65-1.outer.space**
  - antares-esxi65-2.outer.space
- deneb-vc60.outer.space (1)
  - deneb-esxi60-04.outer.space

Automatic checks

Object	Finding description	Finding value
antares-esxi65-1.outer.space	Host version	VMware ESXi 6.5.0
	Host build number	5310538

Major	Network	vSphere	5	Restrict port-level configuration overrides on VDS : vNetwork.restrict-port-level-overrides	Fail
Major	Compute	vSphere	3	Set DCUI.Access to allow trusted users to override lockdown mode: set-dcui-access	Fail
Major	Compute	vSphere	3	Set the count of maximum failed login attempts before the account is locked out: ESXi.set-account-lockout	Fail
Major	Compute	vSphere	1	Set the time after which a locked account is automatically unlocked: ESXi.set-account-auto-unlock-time	Fail
Major	Compute	vSphere	3	Use Active Directory for local user authentication: enable-ad-auth	Fail

Issues in logs

Runecast

CONTEXT

All vCenters

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices
- Security Hardening

LOG ANALYSIS

- Log KBs Discovered
- Log Inspector

Analyze now

Log KBs Discovered

November 20, 2018 - November 27, 2018

Severity | Applies to | Products | Search

Severity	Applies to	KB id	Products	Objects	Last seen date	Description
Major	VM	KB2108710	vSphere	6	17:40 November 25, 2018	The virtual machine fails to start with the error: msg.vmx.poweron.failedErrorCode (2108710)
Major	Compute	KB2145106	vSphere		17:40 November 25, 2018	ESXi 6.x host is disconnected from vCenter Server (2145106)

Details | Findings

Objects	Timestamp	Program
Antares-esxi65-2 (10.3.100.102)	2018-11-22 17:40:20	sshd
Deneb60-3 (10.3.101.103)	2018-11-25 17:40:18	sshd
Deneb60-2 (10.3.101.102)	2018-11-25 17:40:23	sshd
Antares-esxi65-1 (10.3.100.101)		
Antares-esxi65-3		

Showing 3 of 3

ng command 'Error interacting with configuration file /etc/vmware/lunTimestamps.log'
ng command 'Error interacting with configuration file /etc/vmware/lunTimestamps.log'
ng command 'Error interacting with configuration file /etc/vmware/lunTimestamps.log'

Show 25 entries

Showing 1 to 2 of 2 entries

1

Log inspector

Runecast

CONTEXT

All vCenters

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices
- Security Hardening

LOG ANALYSIS

- Log KBs Discovered
- Log Inspector

Analyze now

Log Inspector

SCSI_command | Search for string in Syslog-message... | November 26, 2018 - November 27, 2018

H:0x0 D:0x2 P:0x0 | nmp_ThrottleLogForDevice

Timestamp	Hostname	Program	Syslog-message
21:36 November 26, 2018	deneb-esxi60-04	vmkernel	0:32999)NMP: nmp_ThrottleLogForDevice:3298: Cmd 0x85 (0x439d801f9600, 34426) to dev "mpx.vmhba1:C0:T1:L0" on path "vmhba1:C0:T1:L0" Failed: H:0x0 D:0x2 P:0x0 Va...
21:36 November 26, 2018	deneb-esxi60-04	vmkernel	u0:33000)ScsiDeviceIO: 2651: Cmd(0x439d801f9600) 0x4d, CmdSN 0x51d5 from world 34426 to dev "mpx.vmhba1:C0:T1:L0" failed H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x...
21:36 November 26, 2018	deneb-esxi60-04	vmkernel	cpu1:33141)NMP: nmp_ThrottleLogForDevice:3298: Cmd 0x1a (0x439d801f9600, 0) to dev "mpx.vmhba1:C0:T1:L0" on path "vmhba1:C0:T1:L0" Failed: H:0x0 D:0x2 P:0x0 Valid se...
21:36 November 26, 2018	deneb-esxi60-04	vmkernel	cpu1:32786)NMP: nmp_ThrottleLogForDevice:3298: Cmd 0x1a (0x439d801f9600, 0) to dev "mpx.vmhba0:C0:T0:L0" on path "vmhba0:C0:T0:L0" Failed: H:0x0 D:0x2 P:0x0 Valid se...
21:31 November 26, 2018	deneb-esxi60-04	vmkernel	cpu1:32786)NMP: nmp_ThrottleLogForDevice:3298: Cmd 0x1a (0x439d801f9c00, 0) to dev "mpx.vmhba0:C0:T0:L0" on path "vmhba0:C0:T0:L0" Failed: H:0x0 D:0x2 P:0x0 Valid se...
21:31 November 26, 2018	deneb-esxi60-04	vmkernel	cpu1:32815)NMP: nmp_ThrottleLogForDevice:3298: Cmd 0x1a (0x439d801f9c00, 0) to dev "mpx.vmhba1:C0:T1:L0" on path "vmhba1:C0:T1:L0" Failed: H:0x0 D:0x2 P:0x0 Valid se...

@timestamp	21:36 November 26, 2018
hostname	deneb-esxi60-04
program	vmkernel
message-syslog	cpu0:32999)NMP: nmp_ThrottleLogForDevice:329 ttleLogForDevice
predicate	H:0x0 D:0x2 P:0x0,nmp_ThrottleLogForDevice,nr
issue	SCSI_command,NMP,NMP

Showing 1152 of 1403

vSphere Web Client plugin

Access Runecast Analyzer directly in the vSphere Web Client UI (Flex/Flash and HTML5 versions).

vSphere Client | Menu | Search | ionutr@outer.space | Help

antares-esxi65-1.outer.space | ACTIONS

Summary | Monitor | Configure | VMs | Datastores | Networks | Permissions

- Antares-vC65.outer.space
  - Antares
    - Dev
      - antares-esxi65-1.out...
      - antares-esxi65-2.out...
      - antares-esxi65-3.out...
      - OpsDashboard
        - OpsDB
        - OpsFrontEnd
      - Antares VM1
      - Antares VM2
      - Antares VM3
      - Antares VM4
      - Antares VM5
      - NSX-Controller-1
      - Runecast Analyzer

- Issues and Alarms
  - All Issues
  - Triggered Alarms
  - Alarm Definitions
- Hardware Health
- Performance
  - Advanced
- Tasks and Events
  - Tasks
  - Events
- Runecast
  - Runecast Issues

critical	Knowledge Base	Compute	Availability	vSphere	ESXi host fails with a diagnostic screen due to an Intel Virtualization Technology Erratum (2147325)
critical	Knowledge Base	vCenter	Security	vSphere	Hypervisor-Assisted Guest Mitigation for Branch Target injection (52085)
critical	Knowledge Base	Compute	Security	vSphere	VMware Response to Speculative Execution security issues, CVE-2017-5753, CVE-2017-5715, CVE-2017-5754, and CVE-2018-3693 (aka Spectre and Meltdown) (52245)
critical	Knowledge Base	Compute	Availability	vSphere	ESXi host fails with PSOD after upgrading to 6.5 (2151749)

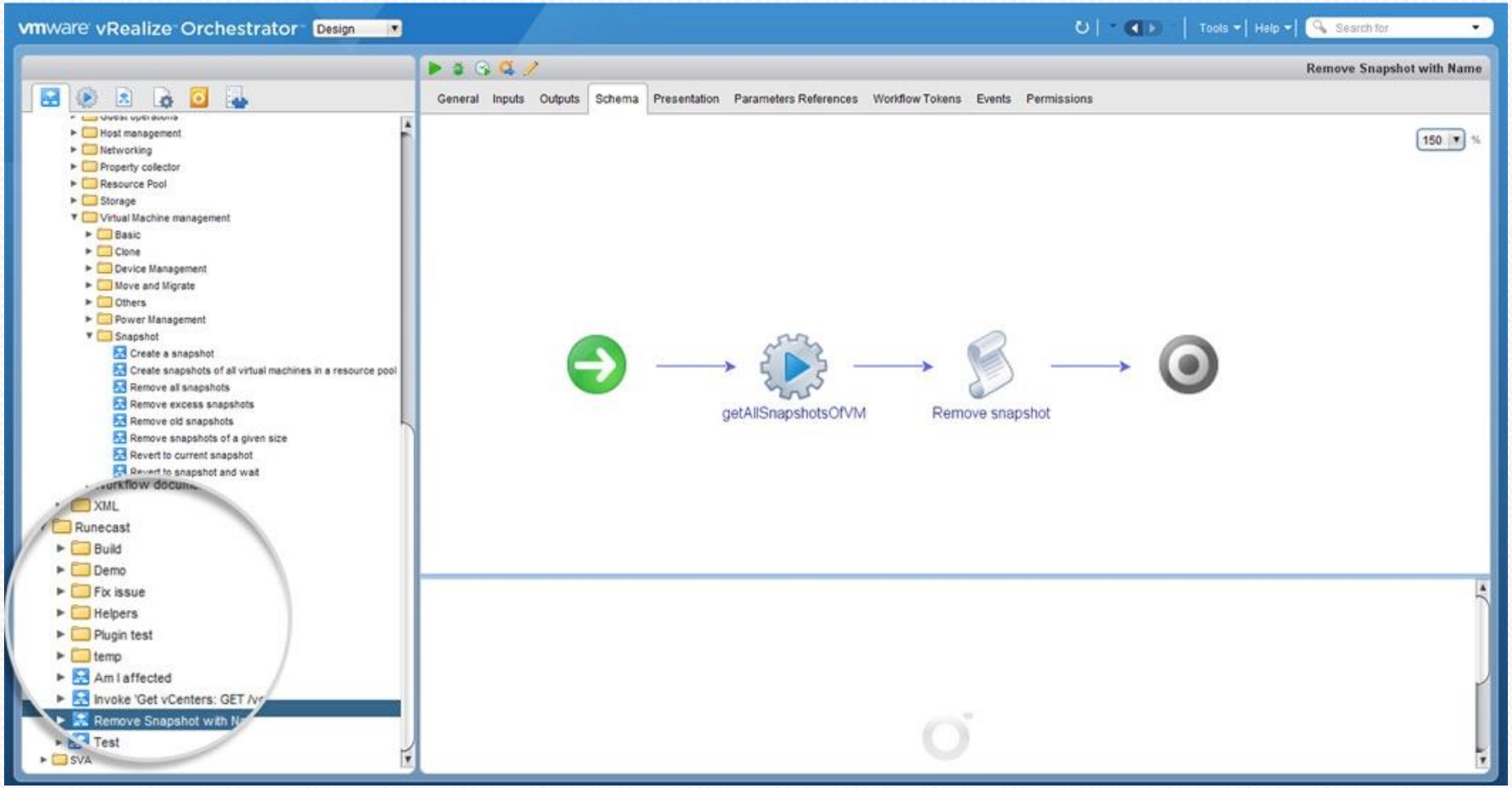
Details | Affected Objects

Object	Findings	
antares-esxi65-1.outer.space	Host NetQueue status	Enabled
	Host build number	5310538
	Host has 10 Gigabit Ethernet adapter	vmnic1
	Host has 10 Gigabit Ethernet adapter	vmnic0
	Host version	VMware ESXi 6.5.0

critical	Best Practice	Compute	Security	vSphere	Ensure that NTP service is running and is set to "Start and stop with host"
critical	Best Practice	Compute	Security	vSphere	Disable SSH unless needed for diagnostics or troubleshooting

vRealize Orchestrator plugin

vRO plugin for remediation workflows and automation leveraging Runecast Analyzer



How many issues can you prevent?

DOWNLOAD FREE TRIAL

runecast.com

PRIANTO

Contact Prianto EMEA Runecast value-added distributor for further inquiries!

Thank You! – Let us know how we can assist you.

- Schedule deep dive with your team
- Feedback
- Ideas
- Additional questions

Prianto Hungary and CEE region
Prianto GmbH
Kőér u. 2/A, 1103 Budapest, Hungary

Tel: +36 70 418 7177
Email: oliver.urzica@prianto.com
www.prianto.hu