



Runecast

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com



Proactive SDDC Management

Eray ATLAS

eray.atlas@onlineteknikdestek.com



Acknowledged by experts

2019 FINALIST AWARDS



Best of VMworld Finalist
Virtualization and Cloud Infrastructure Platform



Computing Technology Product Awards
Best Virtualisation Product



Computing Technology Product Awards
Technology Innovator of the Year



Computing Security Excellence Awards
Security Automation



SDC Awards
Digital Transformation Company of the Year



What Leading Business Analysts are Saying

Gartner COOL VENDOR 2020

Gartner Cool Vendors in Performance Analysis for Cloud-Native Architectures 2020;

Padraig Byrne, Josh Chessman, Federico De Silva, Pankaj Prasad, Charley Rich;

18 May 2020.



Runecast named by Gartner as a "Cool Vendor" in Performance Analysis for Cloud-Native Architectures, 2020

Disclaimer: The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Agenda

- Corporate Footprint and History
- APAC Strategy and Opportunity
- The Business Problem
 - Common Operational Themes
 - SDDC issues in the Environment
- Runecast Solution Overview
 - Business Benefits
 - Selling and Partnering
 - Licensing
- Customer Success Stories

Common Operational Tasks IT Ops face



Which patches apply to which infrastructure stack?

Running different server Hardware, and ESXi versions result in different patch requirements



How do I eliminate bugs that can knock over my environment?

Purple screen of deaths are evident in many critical KB's, downtime cost



Am I meeting the current VMware support matrix? Can I upgrade?

Qualifying each server takes 5-10 mins each, new updates and changes require requalification.



Which solution is the right one?

Hours spent trying to find something that hasn't happened yet, understanding it and adopt the right solution, sometimes there are multiple solutions



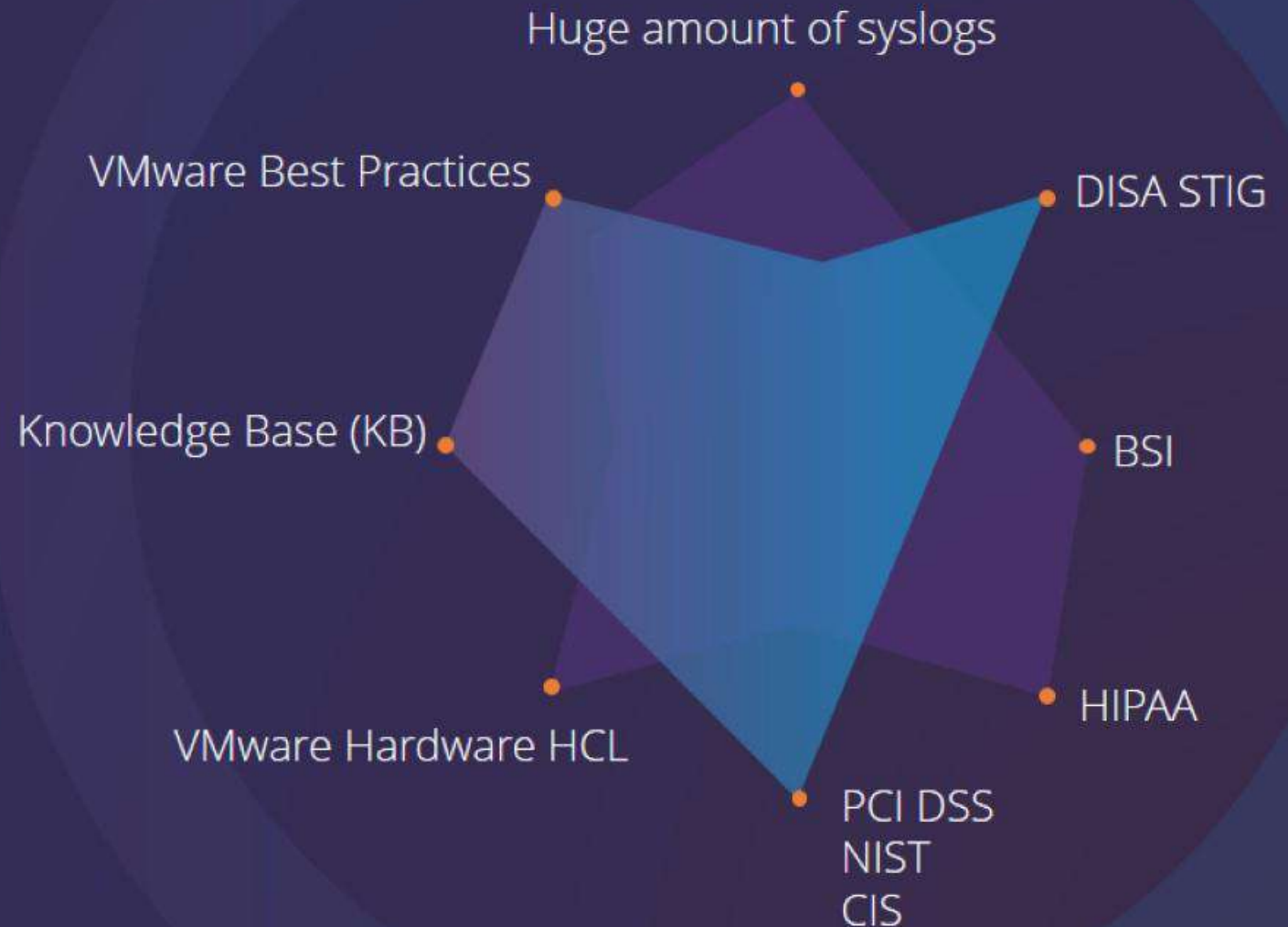
Is my environment performing and secure?

New best practices, tuning for performance, security breaches that appear, security audits – Compliant

Typical problems in a VMware SDDC

Knowledge Base (KB)
Supported H/W config
Best Practices
Security Compliance
Logs

**All that info but your
environment is a minefield**



Problems in IT operations

Over **90% of issues** already documented but used reactively!

human written knowledge sources (documentation, knowledge bases, blog articles, social media)



Break/Fix reactive troubleshooting



Manual Security Compliance efforts



Best Practices **not used**



Increasing complexity and decreasing transparency of IT systems; declining efficiency of IT teams



Lack of skills and **more costly mistakes** in public/hybrid cloud setups

Typical troubleshooting

- Service affected
- Time consuming
- Reactive
- Inefficient
- Not addressing the whole environment
- Not addressing other known issues



Your infrastructure

VMware Knowledge Base Articles

 VMware Security hardening guides and white papers

VMware Best Practices

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

Automates
continuous security compliance checks



Solving problems with Runecast Analyzer

- Pro-active
- Service not affected
- Extremely efficient
- Extremely fast
- Addressing all known issues
- Addressing the whole environment
- Supported Hardware config



Your Infrastructure



VMware ESXi, Hyper-V, KVM, Xen, PVE, etc.
Best practices, configuration guides and whitepapers



Runecast Analyzer
virtual appliance,
running on premises

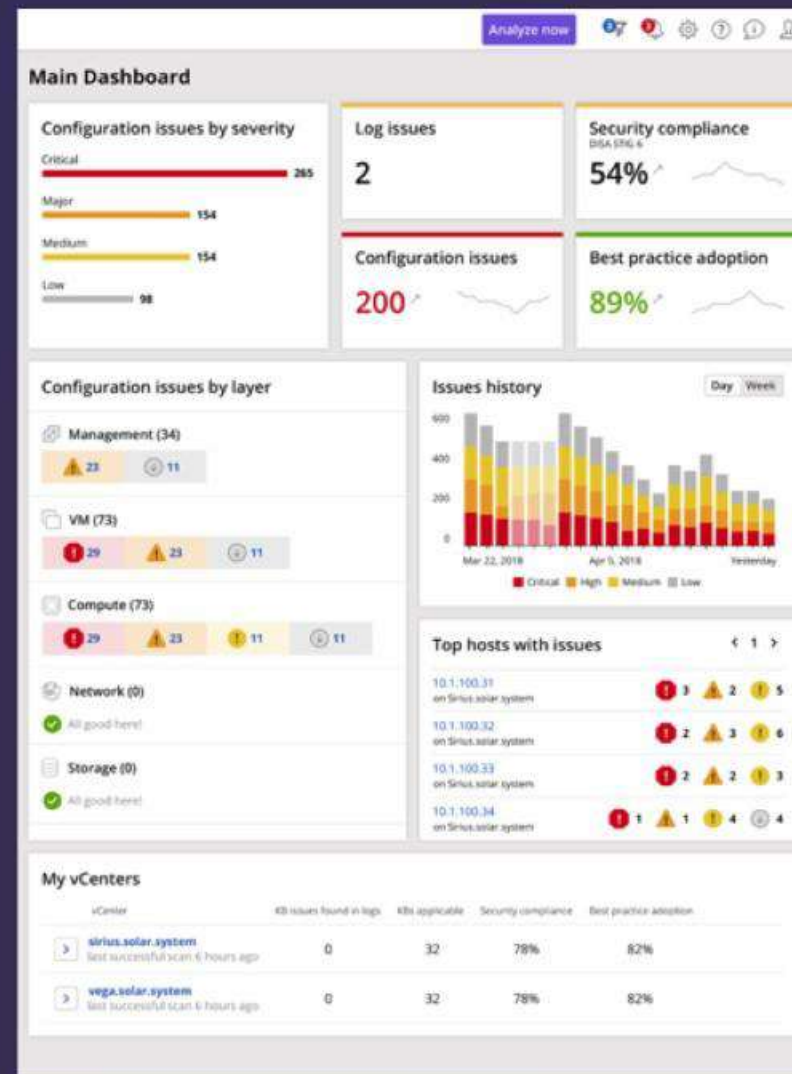
Quick time to value

Download
1 GB OVA

Connect
to vCenters

Analyze
in minutes

- Proactive detection of all known SDDC issues and recommendations
- Automated security compliance (DISA STIG, PCI DSS, HIPAA, BSI, CIS, NIST, GDPR, etc.)
- Eliminates complexity & manual efforts
- Upgrade HCL simulations
- 5-minute deployment, near real-time results, no learning curve
- Secure on-premises architecture, highly scalable with a single virtual appliance.
- Scale out with Enterprise Console for MSPs and dedicated setups



Value



Save time and money

Troubleshooting, health checking, upgrade planning, hiring external resources.



Achieve higher availability

Detect issues before they happen



Automate Security Compliance auditing & reporting

Automate security compliance across the Hybrid Cloud

Use 1 compliance platform for your Hybrid Cloud – VMware, AWS, Kubernetes!

A few key technical features

Deploy and configure 5 to 10 minutes ●

● Never uploads customer data/self contained

Deploys as an OVA file lightweight virtual app ●

● Easy-to-use

vSphere versions (5.x - 7.x) and combinations ●

● Full REST API

vCenter, vSAN, NSX-V and Horizon ●

● vRealize Orchestrator plugin

Kubernetes (including AWS (EKS), Azure (AKS) and Google Cloud (GKE)) ●

● vSphere Web Client plugin

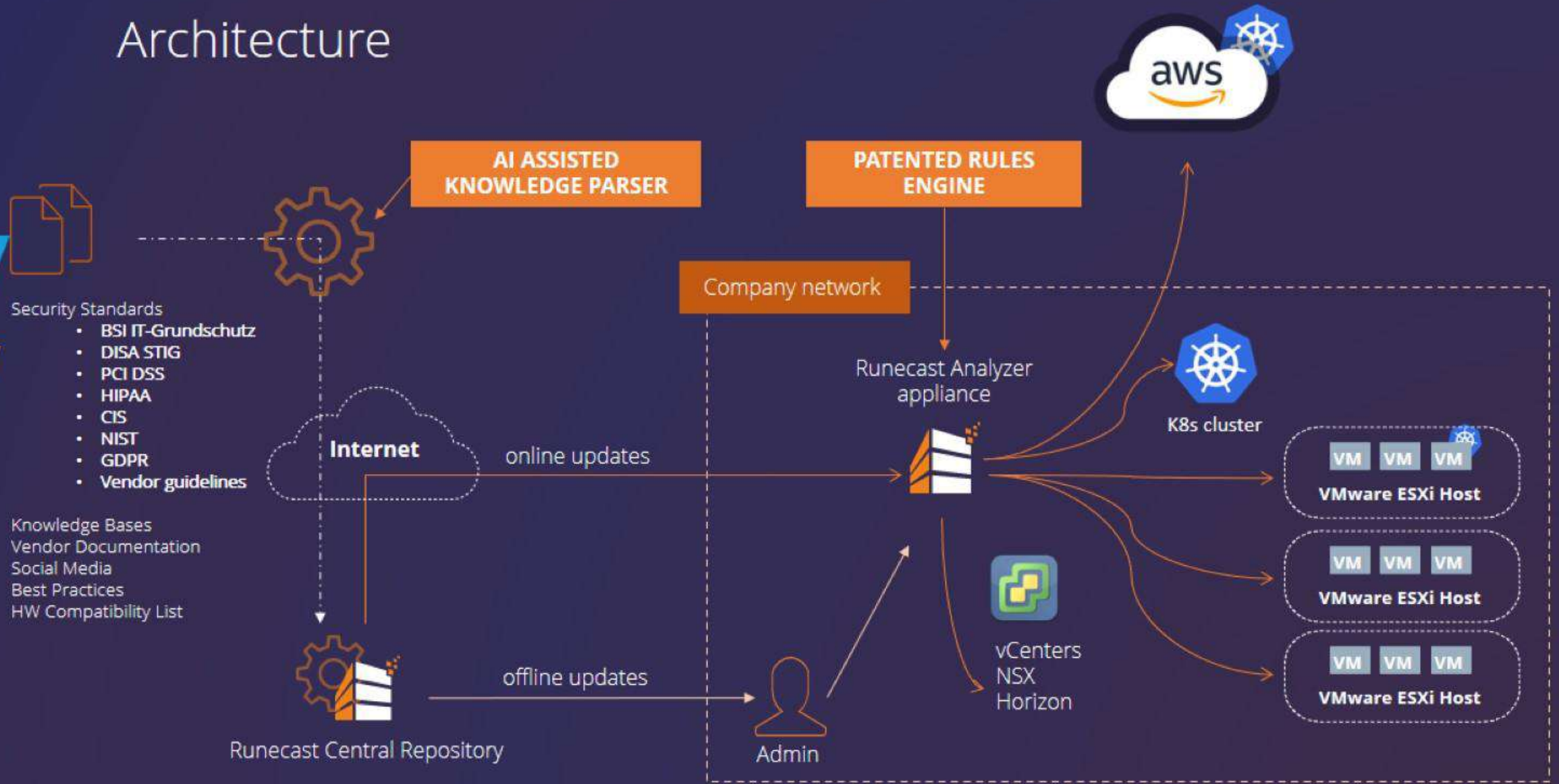
AWS certified for VMware Cloud on AWS ●

● Insights for public cloud AWS

Pure Storage Best Practices for VMware ●

● SAP HANA Best Practices for VMware

Architecture



vRO plugin for auto-remediation & vSphere Web Client plug-in

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.



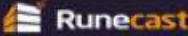
Reduce costs

Prevent outages, save time and avoid audit penalties.



Demo

Health Check in seconds


CONTEXT

All Systems

MAIN MENU

Dashboard

Inventory View

All Issues View

CONFIGURATION ANALYSIS

Config KBs Discovered

Best Practices

Security Compliance

HW Compatibility

LOG ANALYSIS

Log KBs Discovered

Log Inspector

Definition Database

Demo version

DOWNLOAD FREE TRIAL

30

Settings

Help

Export


Search

Config KBs Discovered

Severity	Applies to	Affects	Products	Objects	Title
Critical	Compute	Availability	vSphere	3	"RSSPlugCleanupRSSEngine@lib_netqueue_bal)" purple diagnostic screen on ESXi 6.7 (58874)
Critical	Compute	Availability	vSphere	6	An ESXi host might crash while closing VMware vSphere VMFS6 volumes (59262)
Critical	Compute	Availability	vSphere	2	ESXi 6.0 Update 2 host fails with a PSOD error mentioning Vmxnet3VMKDevRxWithLock (2144968)
Critical	Compute	Availability	vSphere	6	ESXi 6.5 and 6.7 host fails with a PSOD PF Exception 14 in world xxxxx:Unmap Helper IP (70607)
Critical	Compute	Availability	vSphere	3	ESXi 6.5 host crashes PSOD "FS3_ZeroExtents File_FileBlockUnmap FSSVec_FileBlockUnmap" (50114133)
Critical	Compute	Availability	vSphere	3	ESXi 6.5 host crashes with PSOD error "Net_TcpipSetNetStackInstance@vmkernel" (2151545)
Critical	Compute	Availability	vSphere	3	ESXi 6.5 host fails with a PSOD: pcpu 45 Heartbeat NMI (2151597)
Critical	Compute	Availability	vSphere	3	ESXi 6.x crashes with a PSOD - PF Exception 14 in world 65688:HELPER_IMMEDIATE IP (76613)
Critical	Compute	Availability	vSphere	3	ESXi 6.x vSAN host experiences a purple diagnostic screen at bora/modules/vmkernel/isomcommon/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	2	ESXi host 6.0 crashes with PSOD (2150292)
Critical	Compute	Availability	vSphere	3	ESXi host fails with PSOD after upgrading to 6.5 (2151749)
Critical	Compute	Availability	vSphere	1	ESXi host fails with a PSOD "no heartbeat" (67749)
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/dmialloc.c:xxxx - Corruption in dmialloc (2147888)
Critical	vCenter	Security	vSphere	12	Hypervisor-Assisted Guest Mitigation for Branch Target Injection (52085)
Critical	Compute	Security	vSphere	13	Implementing Hypervisor-Specific Mitigations for Microarchitectural Data Sampling (MDS) Vulnerabilities: Concurrent-context attack vector (CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, and CVE-2019-11091) in vSphere (67577)
Critical	Compute	Security	vSphere	13	Implementing Hypervisor-Specific Mitigations for Microarchitectural Data Sampling (MDS) Vulnerabilities: Sequential-context attack vector (CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, and CVE-2019-11091) in vSphere (67577)
Critical	Compute	Security	vSphere	12	L1 Terminal Fault - VMM (L1TF - VMM: Concurrent-context attack vector) Speculative-Execution vulnerability in Intel processors (55806)
Critical	Compute	Security	vSphere	12	L1 Terminal Fault - VMM (L1TF - VMM: Sequential-context attack vector) Speculative-Execution vulnerability in Intel processors (55806)
Critical	Compute	Availability	vSphere	10	PSOD: #PF Exception 14 in world #####:VoI3JournalE (60406)
Critical	Compute	Availability	vSphere	1	PSOD error: "VMKAPI-char-metadata heap at maximum" in the ESXi 6.0 host (2145654)

Send us a message

Drill down

 **Runecast**

ENTERPRISE CONSOLE

EC Dashboard

CONTEXT

All Systems

MAIN MENU

[Dashboard](#)

[Inventory View](#)

[All Issues View](#)

CONFIGURATION ANALYSIS

[Config KBs Discovered](#)

[Best Practices](#)

[Security Compliance](#)

[HW Compatibility](#)

LOG ANALYSIS

[Log KBs Discovered](#)

[Log Inspector](#)

Analyze now

20

Export

Search

Config KBs Discovered

Severity Applies to Affects Products (1)

Filters Applied: Horizon x Clear All

Severity

Applies to

Affects

Critical

VM

Security

Critical

Management

Security

Horizon

vSphere

vSAN

NSX-V

Horizon

Objects

Title

Issue ID

1

VMware Security Advisory: VMSA-2018-0019 (Horizon 6, 7, Horizon Agent, and Horizon Client for Windows updates address an out-of-bounds read vulnerability)

VMW-KB-732

1

VMware Security Advisory: VMSA-2019-0003 (VMware Horizon update addresses Connection Server information disclosure vulnerability)

VMW-KB-1708

Details

Findings

Note

Issue ID: VMW-KB-1708

Source: Knowledge base articles

Reference: <https://www.vmware.com/security/advisories/VMSA-2019-0003.html>

Date of last update: 2019-03-14

Applies to: Management

Risk rating: 6

VMSA-2019-0003

VMware Horizon update addresses Connection Server information disclosure vulnerability

VMware Security Advisory

Advisory ID: VMSA-2019-0003

Major

VM

Availability

Horizon

2

Windows guest operating system crashes at vm3dmp.sys with DRIVER_IRQL_NOT_LESS_OR_EQUAL (67243)

VMW-KB-1709

Medium

VM

Manageability

Horizon

2

Keyboard input is repeated unexpectedly on Horizon virtual desktop or hosted application (59631)

VMW-KB-823

Show

25

entries

1 - 4 of 4 entries (filtered from 94 total entries)

1

Get visibility into your whole Inventory

The screenshot displays the Runecast Enterprise Console interface. On the left is a dark sidebar with navigation options: ENTERPRISE CONSOLE, EC Dashboard, CONTEXT (All Systems), and MAIN MENU (Dashboard, Inventory View, All Issues View). Below these are sections for CONFIGURATION ANALYSIS (Config KBs Discovered, Best Practices, Security Compliance, HW Compatibility) and LOG ANALYSIS (Log KBs Discovered, Log Inspector). The main content area is split into two panels. The 'Inventory View' panel on the left shows a tree of objects with a search bar and a 'Show healthy objects' toggle. The tree includes Antares-vc65, NSX Manager (nsx-manager.outter.space), deneb-vc60, vega-vc67, hcs73, and an AWS Account. The 'Issues' panel on the right, titled 'Issues', shows a list of 93 issues. The first issue is 'Critical VMW-BP-644 Running supported NSX version'. Subsequent issues are 'Critical VMW-PCIDSS-579', 'Critical VMW-PCIDSS-112', 'Critical VMW-PCIDSS-752', 'Critical VMW-PCIDSS-1605', 'Critical VMW-PCIDSS-358', 'Critical VMW-PCIDSS-428', and 'Critical VMW-PCIDSS-790'. Each issue entry includes a severity level, a title, and a brief description.

Runecast
ENTERPRISE CONSOLE
EC Dashboard
CONTEXT
All Systems
MAIN MENU
Dashboard
Inventory View
All Issues View
CONFIGURATION ANALYSIS
Config KBs Discovered
Best Practices
Security Compliance
HW Compatibility
LOG ANALYSIS
Log KBs Discovered
Log Inspector

Inventory View

Search in objects

Show healthy objects

- Antares-vc65.outter.space 148 (2.5k)
 - NSX Manager (nsx-manager.outter.space) 93 (2)
 - controller
 - distributed logical switch
 - edge (2)
 - Antares (2.4k)
- deneb-vc60.outter.space 91 (3.9k)
- vega-vc67.outter.space 51 (3.1k)
 - DR (11)
 - SFO (3.1k)
- hcs73.outter.space 4 (10)
 - connection servers (3)
 - HCS73-ISOLATED 3
 - farms
 - pools (7)
 - security servers
 - view composers
- AWS Account 722739181778 86 (932)

Issues

Analyze now 20

Export

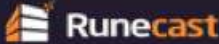
NSX Manager (nsx-manager.outter.space)

Severity: All Source: All More filters Search by title

93 issues

- Critical** VMW-BP-644
Running supported NSX version
BP NSX-V Manageability Network
- Critical** VMW-PCIDSS-579
The NSX Distributed Firewall must be configured to prohibit or restrict the use of unnecessary f... /or services (1.1.4)
PCIDSS NSX-V Security Network
- Critical** VMW-PCIDSS-112
The NSX Distributed Firewall must be configured to prohibit or restrict the use of unnecessary f... /or services (1.2.1)
PCIDSS NSX-V Security Network
- Critical** VMW-PCIDSS-752
The NSX Distributed Firewall must be configured to prohibit or restrict the use of unnecessary f... /or services (1.3.4)
PCIDSS NSX-V Security Network
- Critical** VMW-PCIDSS-1605
The NSX Distributed Firewall must be configured to restrict it from accepting outbound IP packet... h Forwarding (1.3.3)
PCIDSS NSX-V Security Network
- Critical** VMW-PCIDSS-358
The NSX Distributed Firewall must deny network communications traffic by default and allow netwo... y exception) (1.1.4)
PCIDSS NSX-V Security Network
- Critical** VMW-PCIDSS-428
The NSX Distributed Firewall must deny network communications traffic by default and allow netwo... y exception) (1.2.1)
PCIDSS NSX-V Security Network
- Critical** VMW-PCIDSS-790

Best Practices Alignment



CONTEXT

All Systems

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices**
- Security Compliance
- HW Compatibility

LOG ANALYSIS

- Log KBs Discovered
- Log Inspector

Demo version

DOWNLOAD FREE TRIAL

Export


Search

Best Practices

Severity Applies to Affects Products Results

Severity	Applies to	Affects	Products	Objects	Title	Result
Critical	Compute	Security	vSphere	5	Disable SSH unless needed for diagnostics or troubleshooting	Fail
Critical	Compute	Security	EC2	2	Ensure no security groups allow incoming connections from 0.0.0.0/0 to ALL ports and protocols	Fail
Critical	Compute	Security	vSphere	10	Ensure that NTP service is running and is set to "Start and stop with host"	Fail
Critical	Network	Manageability	NSX-V	2	Running supported NSX version	Fail
Critical	Network	Manageability	NSX-V	1	Use supported NSX Controller cluster configuration	Fail
Major	Compute	Performance	vSphere	1	Ensure consistent memory size across hosts in a cluster	Fail
Major	Compute	Availability	vSphere	10	Ensure redundancy for each portgroup	Fail
Major	Compute	Security	vSphere	9	Set timeouts for ESXi Shell and SSH sessions	Fail
Major	VM	Security	vSphere	56	Allow only one remote console session at a time	Fail
Major	Compute	Manageability	vSphere	10	Apply ESXi patches	Fail
Major	Management	Manageability	Horizon	2	Apply Horizon patches	Fail
Major	Network	Manageability	NSX-V	2	Apply NSX Manager patches	Fail
Major	Management	Manageability	vSphere	3	Apply vCenter Server patches	Fail
Major	VM	Performance	SAP HANA, vSphere	2	Configure Paravirtual SCSI Controllers	Fail
Major	VM	Performance	Horizon	2	Configure VDI machines with VMXNET3 adapter	Fail
Major	Network	Availability	NSX-V	1	Configure periodic backup of NSX Manager	Fail
Major	Management	Security	Horizon	1	Configure persistent event logging	Fail
Major	Compute	Performance	vSphere	10	Consistent Hyperthreading configuration	Fail
Major	Management	Manageability	Horizon	1	Deploy at least two Connection Servers	Fail

Automate Security Compliance



ENTERPRISE CONSOLE

EC Dashboard

CONTEXT

All Systems

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices
- Security Compliance**
 - VMware Guidelines
 - DISA STIG
 - PCI DSS
 - HIPAA
 - BSI IT-Grundschutz
 - CIS
 - NIST**

Definition Database

Analyze now

Export

Search

Security Compliance | NIST

Applies to Products Priority Controls Results

Title	Issue ID	Applies to	Products	Objects	Priority	Controls	Result
Configure periodic backup of NSX Manager	VMW-NIST-2427	Network	NSX-V	1	P1	AC-2	Fail
Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	AWS-NIST-2546	Management	CloudWatch	1	P1	AC-2g	Fail
Ensure a log metric filter and alarm exist for CloudTrail configuration changes	AWS-NIST-2545	Management	CloudWatch	1	P1	AC-2g	Fail
Ensure a log metric filter and alarm exist for IAM access key creation.	AWS-NIST-2557	Management	CloudWatch	1	P1	AC-2g	Fail
Ensure a log metric filter and alarm exist for IAM policy changes	AWS-NIST-2544	Management	CloudWatch	1	P1	AC-2g	Fail
Ensure a log metric filter and alarm exist for changes to Network Access Control Lists (NACL)	AWS-NIST-2548	Management	CloudWatch	1	P1	AC-2g	Fail
Ensure a log metric filter and alarm exist for security group changes	AWS-NIST-2547	Management	CloudWatch	1	P1	AC-2g	Fail
Ensure a log metric filter and alarm exist for unauthorized API calls	AWS-NIST-2542	Management	CloudWatch	1	P1	AC-2g	Fail
Ensure a log metric filter and alarm exist for usage of "root" account	AWS-NIST-2543	Management	CloudWatch	1	P1	AC-2g	Fail
Ensure IAM policies are attached only to groups or roles	AWS-NIST-2555	Management	IAM	6	P1	AC-2 (T)(a), AC-6 (10)	Fail
Ensure S3 bucket access logging is enabled on the CloudTrail S3 bucket	AWS-NIST-2540	Storage	S3	2	P1	AC-2g, AU-2c	Fail
The ESXi host must use approved encryption to protect the confidentiality of remote access sessions	VMW-NIST-2275	Compute	vSphere	10	P1	AC-2, SC-13	Fail
Choose "Load Balance - SRCID" for the VXLAN vmknic teaming policy: use-srcid-lb-option	VMW-NIST-2432	Network	NSX-V	1	P1	AC-4	Fail
The distributed port group Forged Transmits policy must be set to reject	VMW-NIST-2393	Network	vSphere	1	P1	AC-4	Fail
The system must ensure the distributed port group MAC Address Change policy is set to reject	VMW-NIST-2394	Network	vSphere	1	P1	AC-4	Fail
The system must ensure the distributed port group Promiscuous Mode policy is set to reject	VMW-NIST-2395	Network	vSphere	1	P1	AC-4	Fail
The ESXi host must display consent banner before granting access to the	VMW-NIST-2336	Compute	vSphere	10	P1	AC-7, AC-8	Fail

https://runecast2-demo/rc2/1security_hardening_nist

Upgrades simulations and HW compatibility check

Hardware Compatibility Overview

Last definition update: 9 hours ago

[Leave Feedback](#)

Action Panel

ESXi Compatibility Simulation ON

ESXi 6.7 U2 Simulate

Inventory Filter

- ☐ Antares-vC65.outer.space
 - ☐ Antares
- ☐ deneb-vc60.outer.space
 - ☐ Deneb

OFF Only hosts with issues (7) Export Search

Host															
<div><div>!</div>antares-esxi65-1.outer.space Antares-vC65.outer.space > Antares > Dev</div> <table><tr><td>Model</td><td>Dell Inc., PowerEdge R730</td><td></td></tr><tr><td>CPU</td><td>2 Intel(R) Xeon(R) CPU E5-2698</td><td>></td></tr><tr><td>ESXi Release</td><td>6.7.0, 13006603</td><td></td></tr><tr><td>BIOS</td><td>Dell 2.7.1</td><td></td></tr><tr><td>Devices</td><td>I/O: 1 / 4</td><td></td></tr></table>	Model	Dell Inc., PowerEdge R730		CPU	2 Intel(R) Xeon(R) CPU E5-2698	>	ESXi Release	6.7.0, 13006603		BIOS	Dell 2.7.1		Devices	I/O: 1 / 4	
Model	Dell Inc., PowerEdge R730														
CPU	2 Intel(R) Xeon(R) CPU E5-2698	>													
ESXi Release	6.7.0, 13006603														
BIOS	Dell 2.7.1														
Devices	I/O: 1 / 4														
<div><div>!</div>antares-esxi65-2.outer.space Antares-vC65.outer.space > Antares > Dev</div> <table><tr><td>Model</td><td>Dell Inc., PowerEdge R730</td><td></td></tr><tr><td>CPU</td><td>2 Intel(R) Xeon(R) CPU E5-2698</td><td>></td></tr><tr><td>ESXi Release</td><td>6.7.0, 13006603</td><td></td></tr><tr><td>BIOS</td><td>Dell 2.7.1</td><td></td></tr><tr><td>Devices</td><td>I/O: 1 / 4</td><td></td></tr></table>	Model	Dell Inc., PowerEdge R730		CPU	2 Intel(R) Xeon(R) CPU E5-2698	>	ESXi Release	6.7.0, 13006603		BIOS	Dell 2.7.1		Devices	I/O: 1 / 4	
Model	Dell Inc., PowerEdge R730														
CPU	2 Intel(R) Xeon(R) CPU E5-2698	>													
ESXi Release	6.7.0, 13006603														
BIOS	Dell 2.7.1														
Devices	I/O: 1 / 4														
<div><div>!</div>antares-esxi65-3.outer.space Antares-vC65.outer.space > Antares > Dev</div> <table><tr><td>Model</td><td>Dell Inc., PowerEdge R730</td><td></td></tr><tr><td>CPU</td><td>2 Intel(R) Xeon(R) CPU E5-2698</td><td>></td></tr><tr><td>ESXi Release</td><td>6.7.0, 13006603</td><td></td></tr></table>	Model	Dell Inc., PowerEdge R730		CPU	2 Intel(R) Xeon(R) CPU E5-2698	>	ESXi Release	6.7.0, 13006603							
Model	Dell Inc., PowerEdge R730														
CPU	2 Intel(R) Xeon(R) CPU E5-2698	>													
ESXi Release	6.7.0, 13006603														

antares-esxi65-1.outer.space

Antares-vC65.outer.space > Antares > Dev

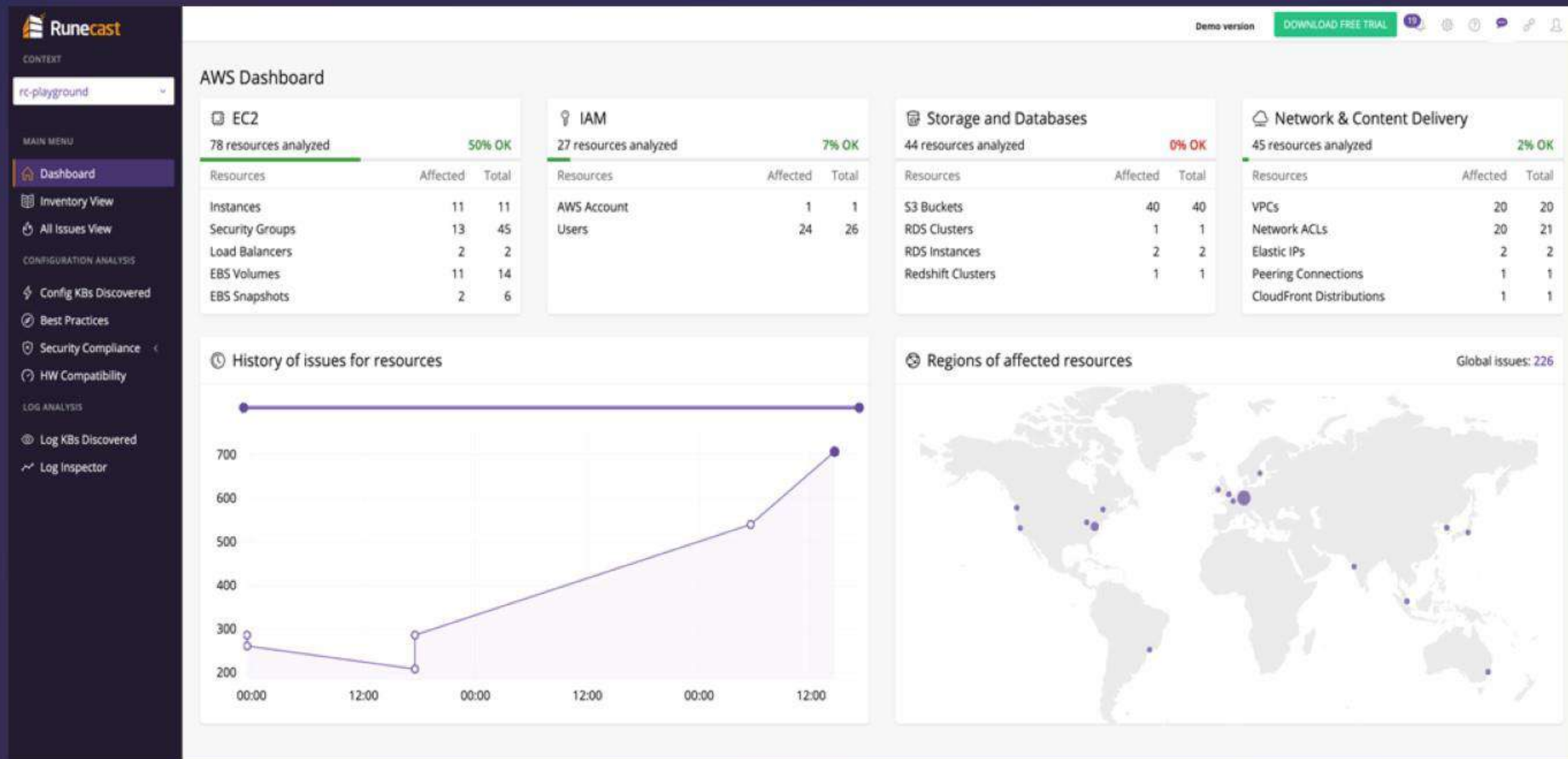
Server ! I/O Devices

Category	Host Data	HCL Data
✓ Partner	Dell Inc.	DELL
✓ Model	PowerEdge R730	PowerEdge R730
✓ CPU Series	Intel(R) Xeon(R) CPU E5-2698 v4 @ 2.20GHz	Intel Xeon E5-2600-v4 Series
✓ Number of Sockets	2	2
⚡ ESXi Release	6.7.0, 13006603	ESXi 6.7 U2
✓ BIOS	Dell 2.7.1	Dell Inc. 2.7.1 UEFI Mode (Boot Mode:UEFI)

HCL Server Notes

The initial version of 'Quick Boot' in VMware vSphere 6.7 will support some configurations of this server. See KB 52477 for details. (<https://kb.vmware.com/s/article/52477>)

Manage AWS Instances



Multi-Tenant Dashboard

EC

CONTEXT

1

MENU

CONFIG

LOG

Analyze now

20

Enterprise Console Dashboard

Data displayed are based on the last successful Analyzer synchronization.

Search

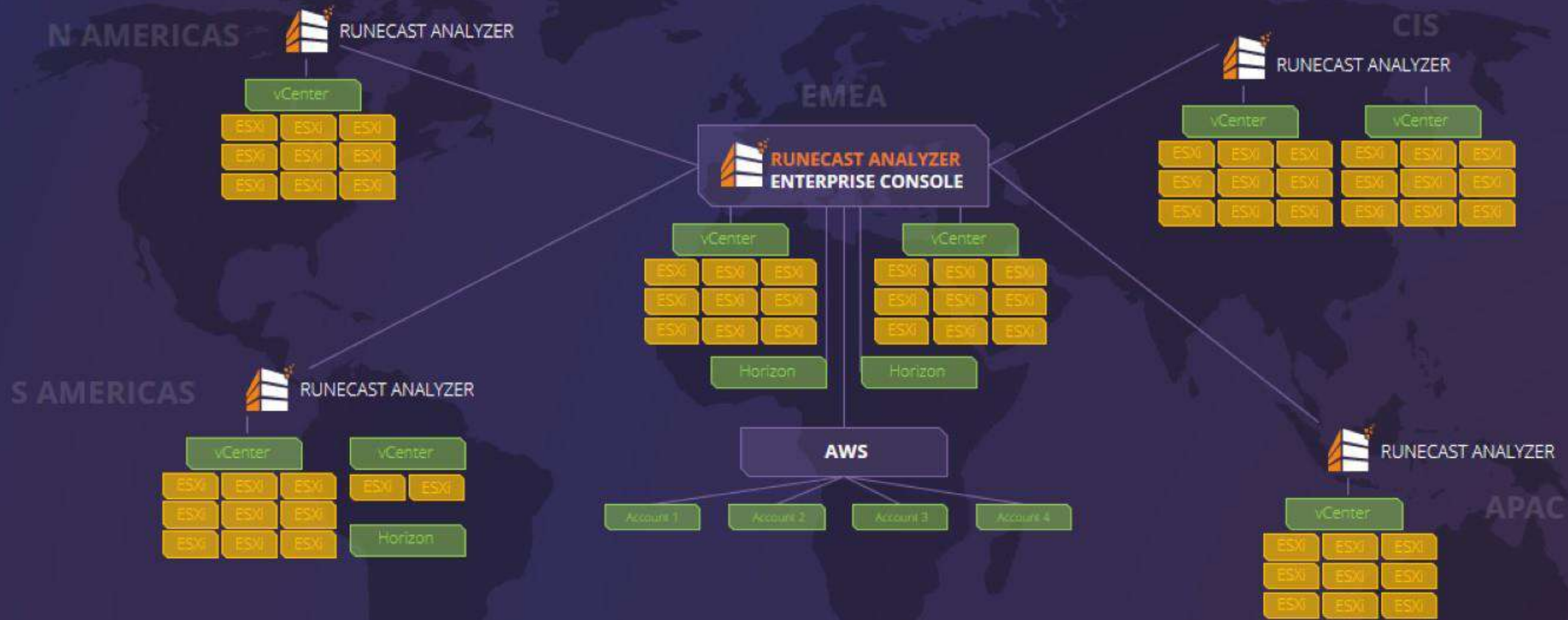
9 systems

Create group

Manage groups

Group		System name	Type	Last analysis	All	Cri	Maj	Med	Low	Log	SC	BP	Sync	Analyzer	Last data retrieved	Version	Edit	
Unassigned	▼	✓ k8s-demo.outer.space	Kubernetes	34 mins	10	C 0	M 9	M 1	L 0	N/A	78%	20%		Local Analyzer	①	4.4.6.0		
Asia	▼	✓ bellatrix-vc.outer.space	vCenter	5 days	59	C 2	M 10	M 17	L 30	N/A	53%	85%	✓	rca-apac.outer.space	①	42 mins	4.4.4.1	
Customer 1	▼	✓ polaris-vc.outer.space	vCenter	2 days	59	C 2	M 10	M 17	L 30	N/A	53%	85%	✓	rca-na.outer.space	①	42 mins	4.4.2.0	
Customer 2	▼	✓ antares-vc65.outer.space	vCenter	31 mins	698	C 53	M 350	M 184	L 111	0	54%	74%		Local Analyzer	①	4.4.6.0		
Customer 2	▼	✓ deneb-vc60.outer.space	vCenter	32 mins	611	C 54	M 290	M 140	L 127	0	54%	78%		Local Analyzer	①	4.4.6.0		
Customer 2	▼	✓ sirius-vc65.outer.space	vCenter	2 days	102	C 31	M 36	M 12	L 23	0	58%	70%	✓	rca-na.outer.space	①	42 mins	4.4.2.0	
Europe	▼	✓ hcs73.outer.space	Horizon	23 hours	9	C 2	M 6	M 1	L 0	N/A	0%	58%		Local Analyzer	①	4.4.6.0		
North America	▼	✓ rc-playground	AWS	23 hours	155	C 25	M 76	M 47	L 7	N/A	25%	3%		Local Analyzer	①	4.4.6.0		
testgroup	▼	✓ vega-vc67.outer.space	vCenter	30 mins	372	C 38	M 243	M 59	L 32	N/A	74%	59%		Local Analyzer	①	4.4.6.0		

Enterprise Console Diagram



vSphere Web Client plug-in

The screenshot displays the vSphere Web Client interface. The top navigation bar includes the 'vSphere Client' logo, a 'Menu' dropdown, a search bar, and user information 'stan@solar.system'. The left sidebar shows a tree view of environments, with 'vega-esxi-1.solar.system' selected under the 'Development' folder. The main content area is divided into several sections:

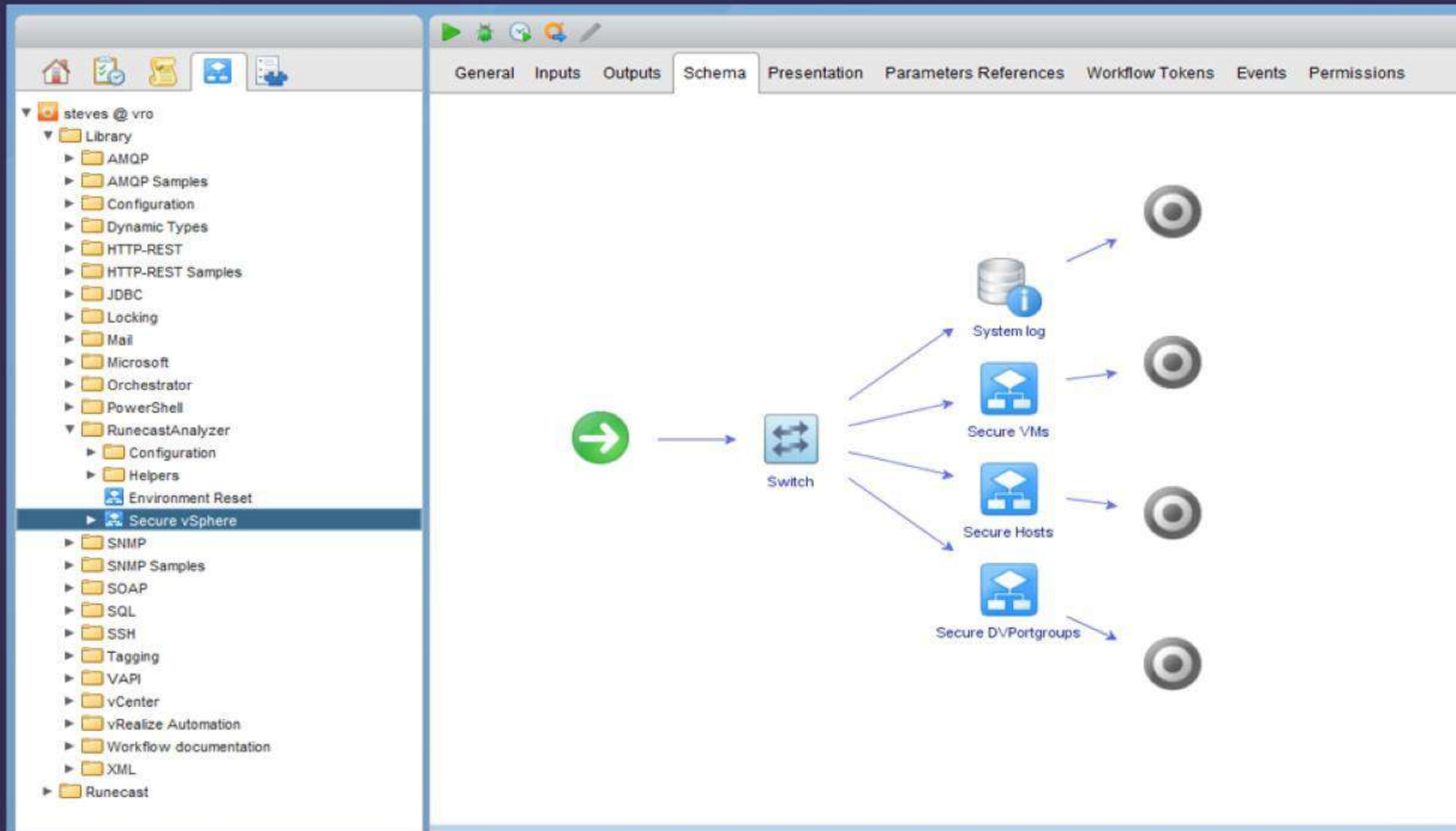
- Summary Tab:** Displays key system information:
 - Hypervisor: VMware ESXi, 6.5.0, 5969303
 - Model: VMware Virtual Platform
 - Processor Type: Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz
 - Logical Processors: 2
 - NICs: 2
 - Virtual Machines: 6
 - State: Connected
 - Uptime: 4 days
- Resource Usage:** Three progress bars showing current usage vs. capacity:
 - CPU:** Used: 225 MHz, Free: 4.38 GHz, Capacity: 4.6 GHz
 - Memory:** Used: 3.33 GB, Free: 2.67 GB, Capacity: 6 GB
 - Storage:** Used: 4.16 GB, Free: 25.83 GB, Capacity: 29.99 GB
- Runecast: Software-Defined Expertise:** A table summarizing issue types and a status message.

Issue Type	Total	Critical	Major	Med/Low
Best Practices	10	2	8	0
Security Hardening	228	11	83	134
Knowledge Base	27	18	6	3

Runecast Analyzer
Scanned on 8/19/2019 at 11:10:27 PM
- Hardware:** A table listing hardware specifications.

Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
CPU	2 CPUs x 2.3 GHz
Memory	3.33 GB / 6 GB
Virtual Flash Resource	0 B / 0 B
Networking	DeathStar-esxi65-15.
Storage	1 Datastore(s)

vRO plug-in





Runecast

Value-Added Distributor
OTD BİLİŞİM
www.otdteknikadestek.com



Kubernetes (NEW)

Explore the Kubernetes Inventory

The screenshot displays the Runecast Enterprise Console interface. On the left is a dark sidebar with navigation options: ENTERPRISE CONSOLE, EC Dashboard, CONTEXT (All Systems), MAIN MENU (Dashboard, Inventory View, All Issues View), CONFIGURATION ANALYSIS (Config KBs Discovered, Best Practices, Security Compliance, HW Compatibility, Custom Profiles), and Definition Database. The main content area is titled 'Inventory View' and includes a search bar, a 'Show healthy objects' toggle, and a tree view of Kubernetes objects. The tree view shows a hierarchy starting with 'k8s-demo.outer.space' (24), which includes 'namespaces' (24). Under namespaces, 'kubernetes-dashboard' (1) is expanded, showing 'network policies' and 'pods' (4). The 'pods' list includes 'dashboard-metrics-scraper-6b4884c9d5-mkwdw' (2) and 'kubernetes-dashboard-7b544877d5-jm6h6' (2). To the right of the inventory view is the 'Issues' section, which shows two issues: a 'Major' issue (K8S-BP-2741) about deployment control and a 'Medium' issue (K8S-BP-2742) about health checks. The interface also features a top navigation bar with an 'Analyze now' button and various utility icons.

Runecast

ENTERPRISE CONSOLE

EC Dashboard

CONTEXT

All Systems

MAIN MENU

Dashboard

Inventory View

All Issues View

CONFIGURATION ANALYSIS

Config KBs Discovered

Best Practices

Security Compliance

HW Compatibility

Custom Profiles

Definition Database

Inventory View

Search in objects

Show healthy objects

- > Antares-vC65.outer.space 150 (2.5k)
- > deneb-vc60.outer.space 92 (3.9k)
- > vega-vc67.outer.space 52 (3.1k)
- > hcs73.outer.space 4 (10)
- > AWS Account 722739181778 86 (932)
- ▼ k8s-demo.outer.space (24)
 - > cluster role bindings
 - > cluster roles
 - ▼ namespaces (24)
 - > default 1
 - > ingress-nginx 1 (7)
 - > kube-node-lease 1
 - > kube-public 1
 - > kube-system 1 (7)
 - ▼ kubernetes-dashboard 1 (4)
 - network policies
 - ▼ pods (4)
 - dashboard-metrics-scraper-6b4884c9d5-mkwdw 2
 - kubernetes-dashboard-7b544877d5-jm6h6 2
 - > role bindings
 - > roles
 - > service accounts
 - pod security policies

Issues

Export


dashboard-metrics-scraper-6b4884c9d5-mkwdw

Severity: All Profile: All More filters Search by title

2 issues

- **Major** K8S-BP-2741
Keep control of your deployment with requests and limits
BP Kubernetes Performance Compute
- **Medium** K8S-BP-2742
Use readiness and liveness probes for health checks
BP Kubernetes Availability Compute

Best practices for K8



ENTERPRISE CONSOLE

EC Dashboard

CONTEXT

All Systems

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices**
- Security Compliance
- HW Compatibility
- Custom Profiles

Analyze now 20

Export

Search

Best Practices

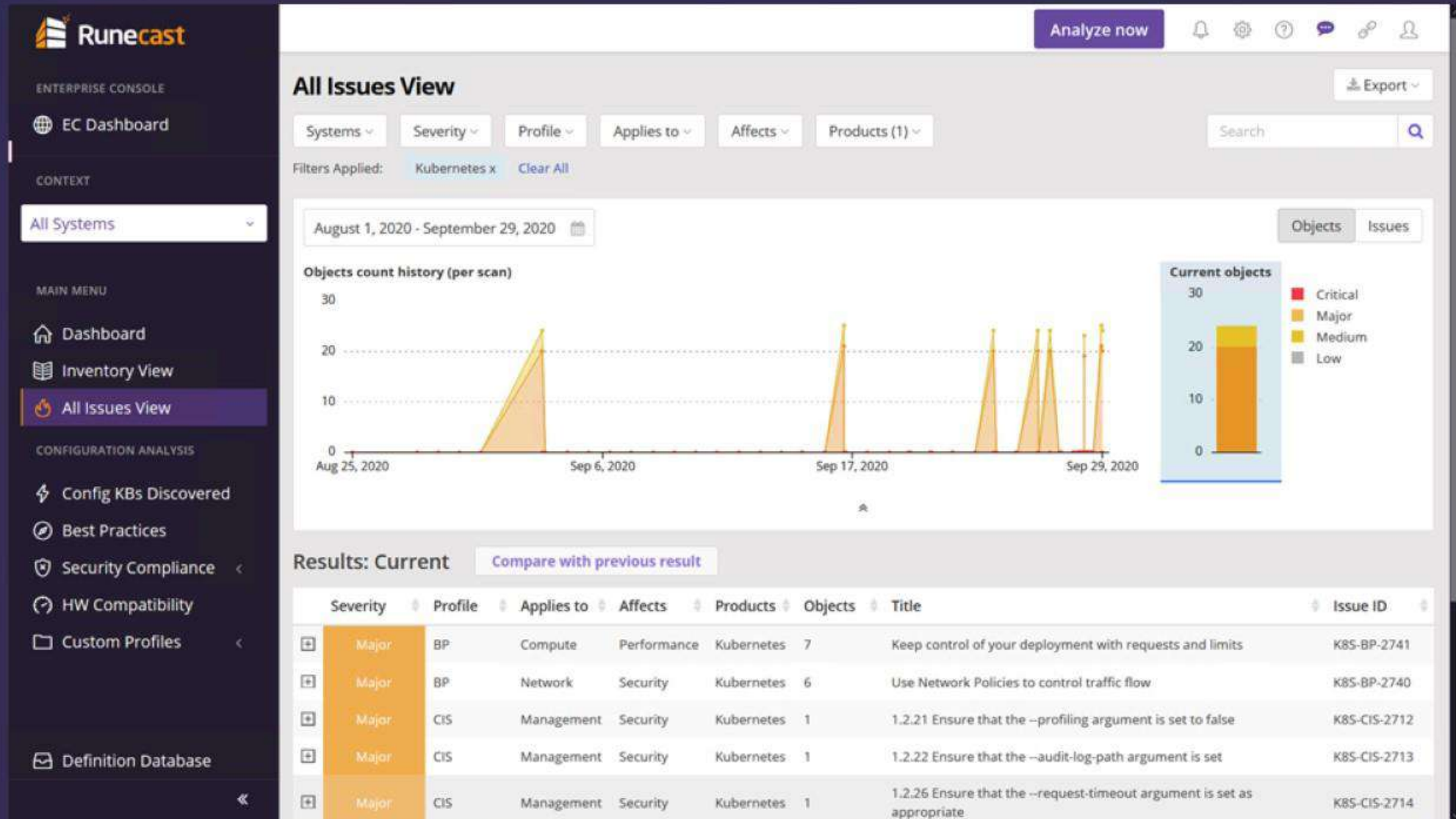
Severity Applies to Affects Products (1) Results

Filters Applied: Kubernetes x Clear All

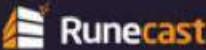
	Severity	Applies to	Affects	Products	Objects	Title	Issue ID	Result
+	Major	Compute	Performance	Kubernetes	7	Keep control of your deployment with requests and limits	K8S-BP-2741	Fail
+	Major	Compute	Security	Kubernetes	1	Enable cluster auditing	K8S-BP-2739	Fail
+	Major	Network	Security	Kubernetes	6	Use Network Policies to control traffic flow	K8S-BP-2740	Fail
+	Medium	Compute	Availability	Kubernetes	4	Use readiness and liveness probes for health checks	K8S-BP-2742	Fail
+	Major	Management	Manageability	Kubernetes	0	Avoid using the 'latest' tag when deploying containers in production	K8S-BP-2743	Pass

Show 25 entries 1 - 5 of 5 entries (filtered from 130 total entries) 1

Historical graph of all K8s issues



Kubernetes CIS Compliance overview



ENTERPRISE CONSOLE

EC Dashboard

CONTEXT

All Systems

All Issues View

CONFIGURATION ANALYSIS

Config KBs Discovered

Best Practices

Security Compliance

- VMware Guidelines
- DISA STIG
- PCI DSS
- HIPAA
- BSI IT-Grundschutz
- CIS
- NIST

Definition Database

Analyze now

Security Compliance | CIS CIS Kubernetes - v1.6.0

Export

Applies to Recommendation Section Level Scored Results

Search

Title	Issue ID	Applies to	Objects	Recommendation Section	Level	Scored	Result
1.2.21 Ensure that the --profiling argument is set to false	K8S-CIS-2712	Management	1	1.2 - Control Plane Components - API Server	L1	Yes	Fail
1.2.22 Ensure that the --audit-log-path argument is set	K8S-CIS-2713	Management	1	1.2 - Control Plane Components - API Server	L1	Yes	Fail
1.2.26 Ensure that the --request-timeout argument is set as appropriate	K8S-CIS-2714	Management	1	1.2 - Control Plane Components - API Server	L1	Yes	Fail
1.2.27 Ensure that the --service-account-lookup argument is set to true	K8S-CIS-2715	Management	1	1.2 - Control Plane Components - API Server	L1	Yes	Fail
1.3.2 Ensure that the --profiling argument is set to false	K8S-CIS-2723	Management	1	1.3 - Control Plane Components - Controller Manager	L1	Yes	Fail
1.4.1 Ensure that the --profiling argument is set to false	K8S-CIS-2728	Management	1	1.4 - Control Plane Components - Scheduler	L1	Yes	Fail
1.2.18 Ensure that the --insecure-bind-address argument is not set	K8S-CIS-2711	Management	0	1.2 - Control Plane Components - API Server	L1	Yes	Pass
1.2.2 Ensure that the --basic-auth-file argument is not set	K8S-CIS-2706	Management	0	1.2 - Control Plane Components - API Server	L1	Yes	Pass

javascript:



Runecast

Value-Added Distributor
OTD BİLİŞİM
www.otdteknikadestek.com



Custom Security Profiles (NEW)

Copy any rule to Custom Profile

Runecast
ENTERPRISE CONSOLE

EC Dashboard

CONTEXT

All Systems

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices
- Security Compliance
- HW Compatibility
- Custom Profiles

Definition Database

Analyze now

Export

Severity Profile Applies to Affects Products Search

Severity	Profile	Applies to	Affects	Products	Title	Issue ID	Updated on
Critical	KB	Compute	Availability	vSphere	Restarting NEC Baseboard Management Controller (BMC) fails with a purple diagnostic screen or ESXi/ESX host becomes unresponsive (2071068)	VMW-KB-1161	2015-12-14
Critical	KB	Compute	Availability	vSphere	ESXi 5.5/6.0.x host loses network connectivity with Broadcom 10 GB Nics and bnx2x driver loaded under heavy VXLAN traffic (2114957)	VMW-KB-1302	2016-06-27
Critical	LOG	Compute	Availability	vSphere	PSOD Can Occur When Using QFLE3 Driver (79058)	VMW-LOG-2588	2020-08-17

Details Note

Issue ID: [VMW-KB-1161](#)

Knowledge profile: Knowledge base articles

Reference: <https://kb.vmware.com/s/article/2071068>

Date of last update: 2015-12-14

Applies to: Compute

Risk rating: 6

Restarting NEC Baseboard Management Controller (BMC) fails with a purple diagnostic screen or ESXi/ESX host becomes unresponsive (2071068)

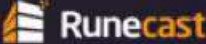
Resolution

This is a known issue when restarting the NEC Baseboard Management Controller (BMC) on a NEC server while the host is running ESXi/ESX.

To prevent this issue, NEC documentation recommends that the BMC not be restarted on a live production system when running ESXi/ESX. Per the NEC documentation, avoid these BMC operations while the VMware hypervisor is running:

- SP Reset

Custom Profiles



ENTERPRISE CONSOLE

EC Dashboard

CONTEXT

All Systems

MAIN MENU

- Dashboard
- Inventory View
- All Issues View

CONFIGURATION ANALYSIS

- Config KBs Discovered
- Best Practices
- Security Compliance
- HW Compatibility
- Custom Profiles**

Definition Database

Analyze now

20

Settings

Help

Chat

Link

User

Custom Profile | ACME Internal Policy

Export

Severity Applies to Affects Products Issue type Results

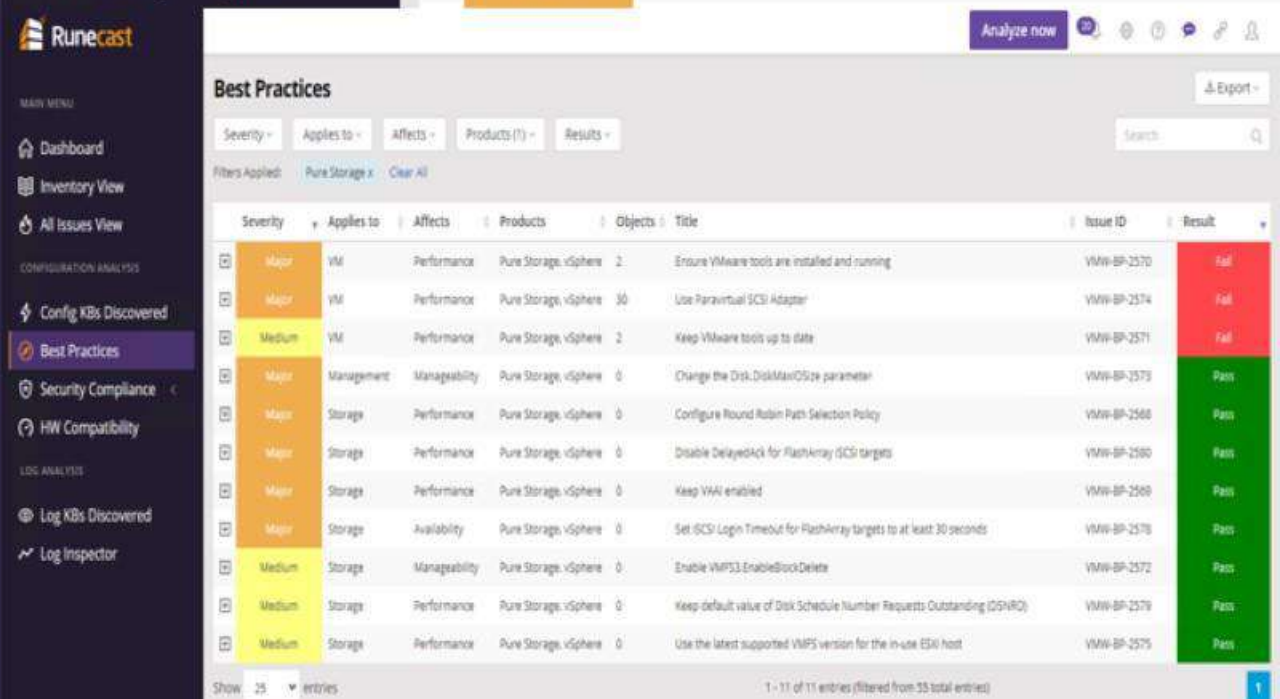
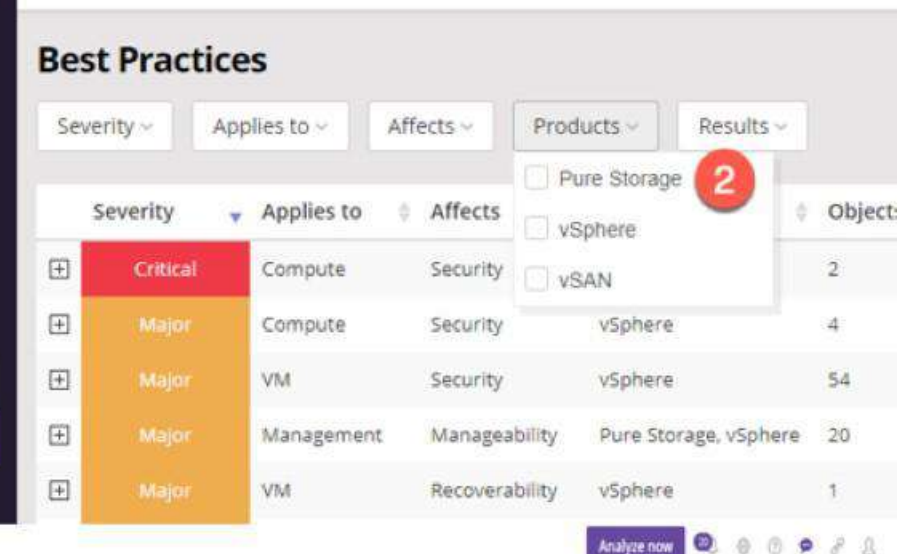
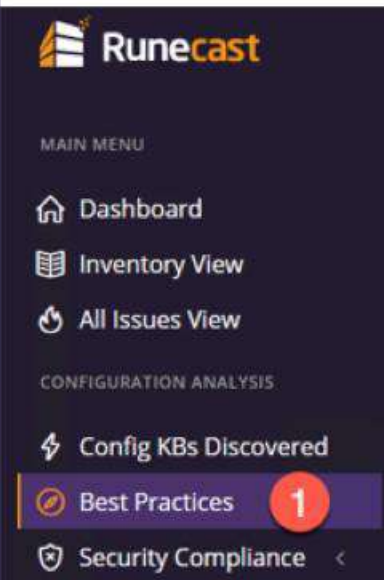
Search

	Severity	Applies to	Affects	Products	Objects	Issue type	Title	Issue ID	Result
+	Critical	Compute	Security	vSphere	10	SH	Configure NTP time synchronization: config-ntp	VMW-ACME-C2	Fail
+	Major	Compute	Performance	Kubernetes	7	BP	Keep control of your deployment with requests and limits	K8S-ACME-C17	Fail
+	Major	Compute	Availability	vSphere	10	BP	Nestle: Ensure redundancy for each portgroup	VMW-ACME-C9	Fail
+	Major	Compute	Availability	vSphere	10	KB	ACME ESXi host might crash with PSOD during shutdown with IPv6 and MLDv1 in physical network (55780)	VMW-ACME-C16	Fail
+	Major	Compute	Availability	vSphere	10	KB	ACME rule is ESXi host might crash with PSOD during shutdown with IPv6 and MLDv1 in physical network (55780)	VMW-ACME-C18	Fail
+	Major	Compute	Manageability	vSphere	10	BP	ACME: Apply ESXi patches for all ACME servers	VMW-ACME-C5	Fail
+	Major	Management	Manageability	vSphere	3	BP	Apply vCenter Server patches for all ACME vCenters	VMW-ACME-C6	Fail
+	Major	Compute	Security	vSphere	1	SH	Disable TLS 1.0 and 1.1 on ESXi Hosts if necessary: ESXi.Disable-oidtls-protocols	VMW-ACME-C3	Fail

NEW:

Pure Storage Best Practices Alignment

- VMware Best Practices for Pure Storage FlashArray Automated Checks
- Maximise your VMware and Pure Storage investment by leveraging the latest Best practices
- Gain improvements in Redundancy, SPOF, Manageability
- Uncover BP gaps in seconds



Companies with happy
admins who benefit from
Runecast intelligence



Success Story: Verizon



- Ongoing issues in their virtual environment – 24 vCenters and approx. 750 hosts
- IT Ops Team was not large enough to stay on top of these issues.
- Large amount of time spent on troubleshooting, patching, firefighting
- Reactive rather than proactive
- Up and running in 15 mins
- Reduced large majority of issues in environment
- Freed up majority of IT team to spend on innovative projects

Case Study

Notino

- Major European eShop Notino reduces VMware Related Incidents by 80%
- Notino reduced OPEX tied to troubleshooting costs, as their team immediately demonstrated savings of one full-time admin, enabling them to focus those savings on additional initiatives.
- Costs Saved FTE– €78K/year
- Data center downtime – €236K/hour



Runecast Case Study

NOTINO

Company

Notino

Website

www.notino.com

Industry

Retail, eCommerce

Location

Prague, Czech Republic

Employees

~1200

Overview

Europe's largest online fragrance and beauty retailer relies on Runecast Analyzer for real-time support and mitigation of datacenter downtime

"Runecast saves us from issues before they happen, the value of which cannot be overstated. In addition, Runecast's real-time data saves us weeks and months that were previously spent on dealing with VMware support."

Major European eShop reduces VMware Related Incidents by 80%

Overview

Notino is the largest online fragrance and beauty retailer in Europe, active in 23 countries and growing. The company provides more than 1,500 brands and 60,000 products, with deliveries to more than 400 million European customers. For three consecutive years, Notino has been awarded by Deloitte as one of the 50 fastest growing technology companies.

By 2017, Notino had over €280M turnover, and a growing ecommerce-driven company requires a stable SDDC to ensure business continuity that can take and dispatch up to 80,000 orders per day throughout the continent.

Michal Kopečný and Jaroslav Toman are IT Administrators at Notino and responsible for the company's VMware infrastructure.

Challenge

With 3 vCenter Servers (managing over 50 ESXi hosts) and a Horizon VDI environment, Notino was experiencing 4-5 VMware-related IT incidents per month, which could be disastrous to a company with roughly half a million daily visits to online shops. Also, the company's presence in 23 countries gave the challenge of needing to find workarounds to fix issues proactively, without the help of on-site VMware support.

According to Mr. Kopečný, "We needed better support, either from VMware or Runecast... and with VMware that would be adding 'mission-critical plus a TAM', which was more expensive than Runecast. Using Runecast gives us the real-time support that we need."



2164R - Kemp House, 152 City Road,
London EC1V 2NX, UK

innovate@runecast.com
www.runecast.com

Testimonials

PRO BTP

customer: PRO BTP

industry: Finance/Construction

location: France

employees: ~6000

PRO BTP utilizes Runecast Analyzer to keep their VMware virtual infrastructure running at optimal performance and enabling their IT department to run more efficiently



"Runecast Analyzer provides us a proactive view of our production vSphere cluster and enables us discover issues that might impact our productivity before they occur. It saved us countless hours of tedious work"

Alexandre Potier
Virtualization Architect
PRO BTP

Testimonials

de Volksbank

customer: de Volksbank

industry: Finance/Banking

location: The Netherlands

employees: ~4800

Increasing uptime for their customer 75% time saved on troubleshooting and root cause analysis Being able to identify and monitor potential risks Being able to mitigate risks in a controlled and non-service affecting manner.

de volksbank

"Our main goal is to serve our customers with a high-end, feature-rich and robust electronic banking environment. With Runecast we can now proactively prevent outages on the systems that provide that environment."

Rob van der Helm
Infrastructure Designer
de Volksbank

Testimonials

ONI

customer: ONI PLC

industry: Managed Service Provider

location: UK, worldwide services

employees: 75

Zero issues/VMware incidents across 5 vCenters and 50+ hosts 70-80% man-hours time savings over 100 issues detected and fixed



"Runecast Analyzer discovered more than 100 issues, some of which were critical (PSOD, open ports, Network driver issues). It reduced our typical 2 issues per month to 0 and saved us lots of time."

Gordon Howes
Cloud Service Manager
ONI

Testimonials

Indonesian Cloud

industry: Cloud Service Provider

location: Indonesia

employees: ~100



"When we started testing Runecast Analyzer, I was amazed by the number of issues we were able to find and resolve in a very short time. The report showed us where the issues were, how to fix them and even prioritized them in an easy to understand form. For example, the issue described in KB1027511 was detected on a number of Linux virtual machines. We could then quickly remediate it and easily improve the network performance over a big number of VMs,

Reza Kertadjaja, Chief Operations Officer.



Runecast

Value-Added Distributor
OTD BİLİŞİM
www.onlineteknikdestek.com



visit <http://runecast.com> to start a 14-day trial and gain results within 15 min



otd.salesgrp@onlineteknikdestek.com



www.onlineteknikdestek.com