

ITOPS-003 – Patch Management

The vulnerability patch scanners were configured in the infrastructure using the AWS System Manager module and its Patch Manager component. Reviewing the Compliance Report for that purpose. For operational reasons, and to avoid installing an update that could affect operational continuity, only the option of patch scan and evaluation of the same was configured, to proceed manually to its installation.

Patch Management:

AWS Systems Manager > Patch Manager > Compliance reporting

Patch Manager [Info](#) [Patch now](#) [Create patch policy](#)

► Overview of patching operations - new

Dashboard **Compliance reporting** Patch baselines Patches Settings

Node patching details (1) [View log](#) [View detail](#) [Export to S3](#) [View all S3 exports](#)

Q

	Name	Node ID	Patch configuration name	Patch configuration type	Compliance status	Critical non-compliant count	Security non-compliant count	Other non-compliant count
<input type="radio"/>	INF-DC	i-0ea2684b3461707d6	infinity-ssm	Patch policy	Compliant	0	0	0

AWS Systems Manager > Patch Manager > Patches

Patch Manager [Info](#) [Patch now](#) [Create patch policy](#)

► Overview of patching operations - new

Dashboard Compliance reporting Patch baselines **Patches** Settings

Operating system
Windows

Patches (650+)

Q Filter patches

< 1 ... 56 57 58 59 60 61 ... >

	KB	Name	Product	Product family	Classification
<input type="radio"/>	KB2267959	Microsoft HealthVault Connection Center v3.0	HealthVault Connection Center	Microsoft HealthVault	Feature
<input type="radio"/>	KB2310138	Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.423.81.0) - Current Channel (Broad)	MS Security Essentials	Microsoft Security Essentials	Definit
<input type="radio"/>	KB2310138	Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.421.1844.0) - Current Channel (Broad)	MS Security Essentials	Microsoft Security Essentials	Definit
<input type="radio"/>	KB2310138	Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.421.1551.0) - Current Channel (Broad)	MS Security Essentials	Microsoft Security Essentials	Definit
<input type="radio"/>	KB2310138	Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.421.1850.0) - Current Channel (Broad)	MS Security Essentials	Microsoft Security Essentials	Definit
<input type="radio"/>	KB2310138	Security Intelligence Update for Microsoft Security Essentials - KB2310138 (Version 1.421.1667.0) - Current Channel (Broad)	MS Security Essentials	Microsoft Security Essentials	Definit



AWS Systems Manager > Patch Manager > Dashboard

Patch Manager [Info](#)

Patch now Create patch policy

Overview of patching operations - new

Dashboard Compliance reporting Patch baselines Patches Settings

Amazon EC2 instance management

Snapshot of EC2 instances in your AWS account that are and are not managed by Systems Manager.

Reporting not enabled

To view the EC2 instance snapshot, enable the Amazon EC2 OpsData source in Explorer and set up recording in AWS Config. [Learn more](#)

Enable Explorer

Compliance summary

Summary of compliance status for managed nodes that have previously reported patch data.

100%

Compliant

Compliant Critical noncompliant High noncompliant Other noncompliant

Noncompliance counts

The number of noncompliant nodes for each of the most common reasons for being out of compliance.

Nodes with missing patches: 0

Nodes with failed patches: 0

Nodes pending reboot: 0

Compliance reports

Count of instances based on the age of their most recent patching compliance reports.

0%

Compliance reported within the past 7 days

Compliance not reported within the past 7 days

Compliance never reported

Patch Manager [Info](#)

Patch now Create patch policy

Patch summary (2453)

View log Export to S3 View all S3 exports

Search for Patches

Name	State	Classification	Severity	Compliance level	Patch configuration name	Patch configuration type	Baseline ID used
KB4558997	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB4562562	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB4566424	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB4570332	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB4577667	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB4587735	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB4598480	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB4601393	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB5000859	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c
KB5001404	Installed	SecurityUpdates	Critical	UNSPECIFIED	infinity-ssm	Patch policy	pb-0057d2461edb17c

Vulnerability Scan with Amazon Inspector:

Inspector > Findings > By instance

Findings: By instance [Info](#)

Sorted by instances with the most critical findings.

By instance (3)

Create suppression rule

Choose a row to view the instance's details and associated findings.

Add filter

EC2 instance	Account	Operating system	Amazon machine image	Critical	High	All
i-0db22a542eab12f58	992382705250	WINDOWS_SERVER_2019	ami-035bb1643e73bcf09	6	134	218
i-0133524837119c69e	992382705250	-	ami-0776705a22f4ba314	0	0	1
i-0ea2684b3461707d6	992382705250	WINDOWS_SERVER_2019	ami-035bb1643e73bcf09	0	110	384



Acknowledgment & Acceptance

Please sign below to acknowledge that you've received, reviewed, and understood the security responsibilities.

Customer Name: _____

Signature: _____

Date: _____