Qualys TotalCloud v2.x

Release Notes

Version 2.7.0
November 20, 2023

What's New

Microsoft Azure

Support for Vulnerability View in the Microsoft Azure Inventory

Common Features

New Insights tab in the TotalCloud Application

New Tokens

Control Changes

Qualys TotalCloud 2.7.0 brings you improvements and updates! Learn More

For updates to the Connector APIs, refer to the Connector API Release Notes

For updates to the Connector Application, refer to the Connector Release Notes

Microsoft Azure

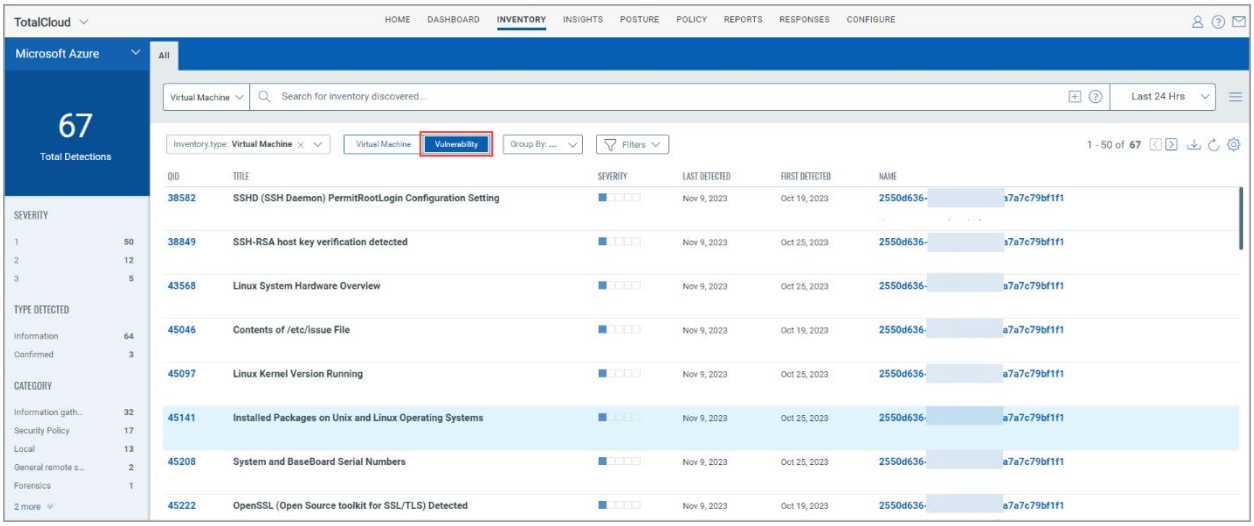
Features introduced to Microsoft Azure in this release.

Support for Vulnerability View in the Microsoft Azure Inventory

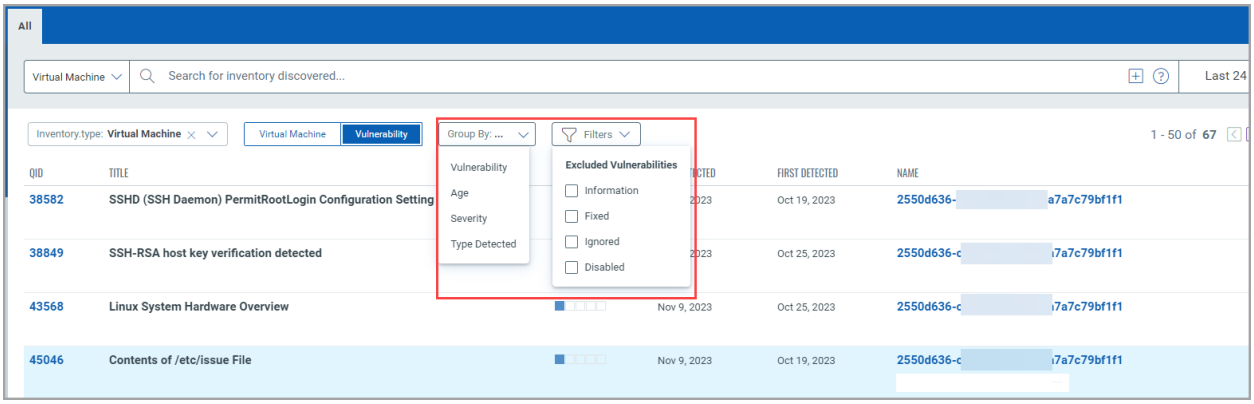
TotalCloud has long since offered the option to view your AWS resources by their detected vulnerabilities, now we are extending support of this key feature to Microsoft Azure.

This enhancement broadens the scope of vulnerability management capabilities and provides a unified view of vulnerabilities across both AWS and Azure platforms.

Navigate your Azure inventory and discover the **Vulnerability** option. With a click, you can access valuable insights into the vulnerabilities that impact your Azure virtual machines.



You can further sort out your searches by clicking **Group By** or **Filter** to modify the Vulnerability list.

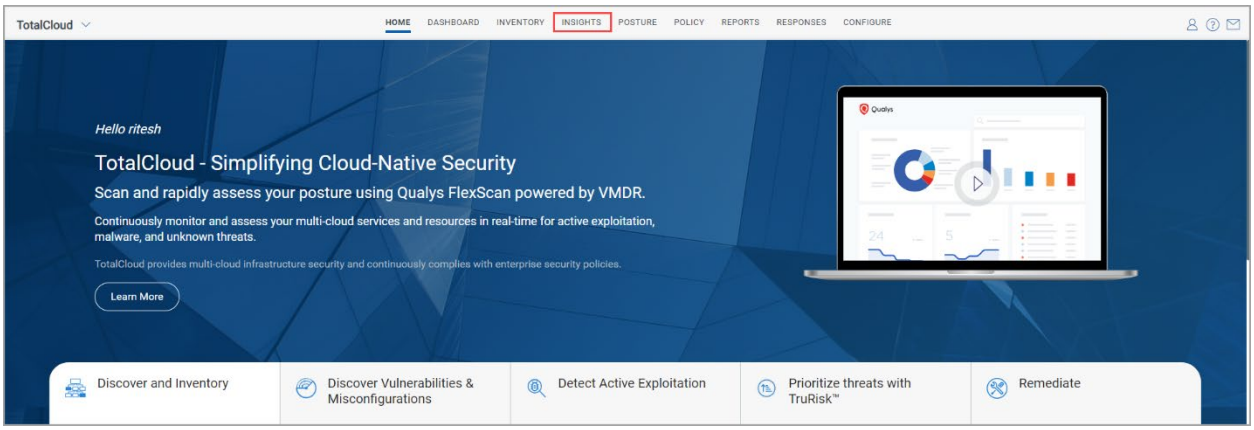


Common Features

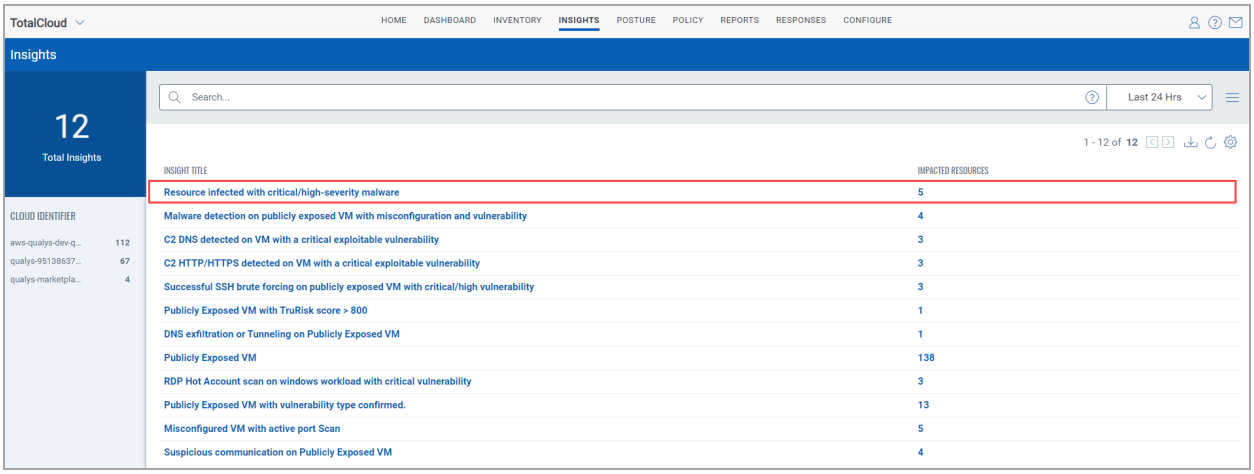
Common Features introduced to the TotalCloud Application in this release.

New Insights tab in the TotalCloud Application

In our latest release, we are excited to introduce a new feature to enhance your TotalCloud experience. Building on the success of our previous TruRisk score feature, TotalCloud 2.7 takes your TruRisk journey to the next level by introducing the all-new **Insights** tab.



The **Insights** tab harnesses the full power of TotalCloud, combining features such as posture analysis, scan results, and CDR results to uncover critical environmental risks across all your cloud accounts. This invaluable information is comprehensively presented to you through a series of reports.

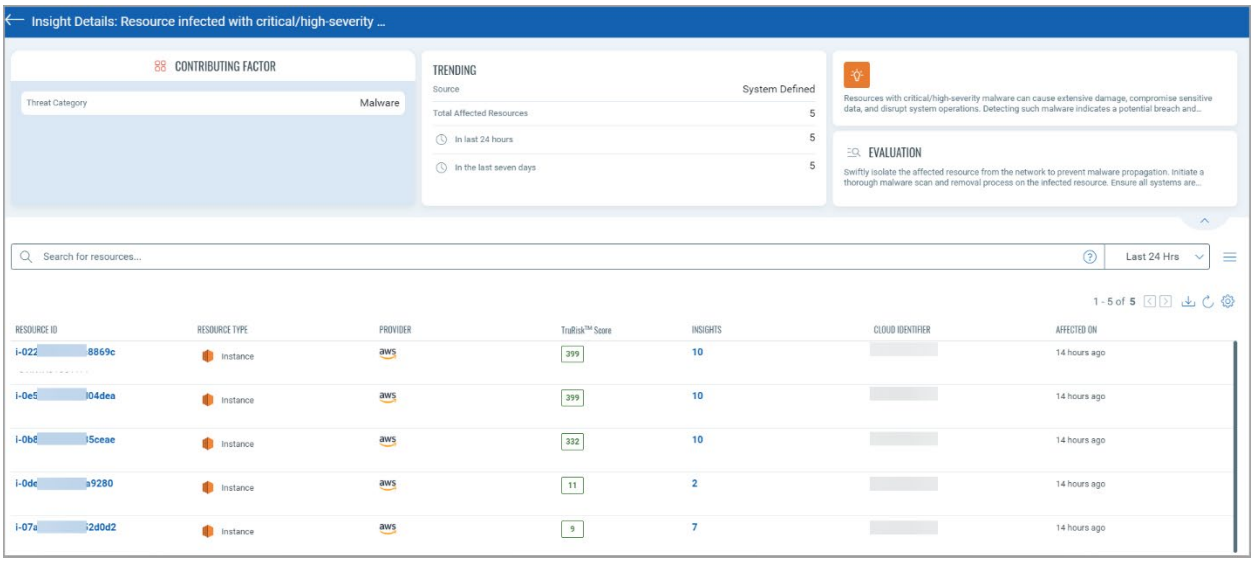


Click the insight title to explore each insight in depth. Gain a clear understanding of its severity, the potential risks it poses, and effective strategies for mitigation.

You can click the count of impacted resources to view the affected resources from the TotalCloud Inventory.

These insights go further by providing a detailed list of risk scenarios, each categorized by severity. As you delve deeper into the insights, you gain information on the specific resources within your cloud accounts that are impacted by these risk scenarios. It identifies the contributing factor and the mitigation method for the Insight. For example, you can discover

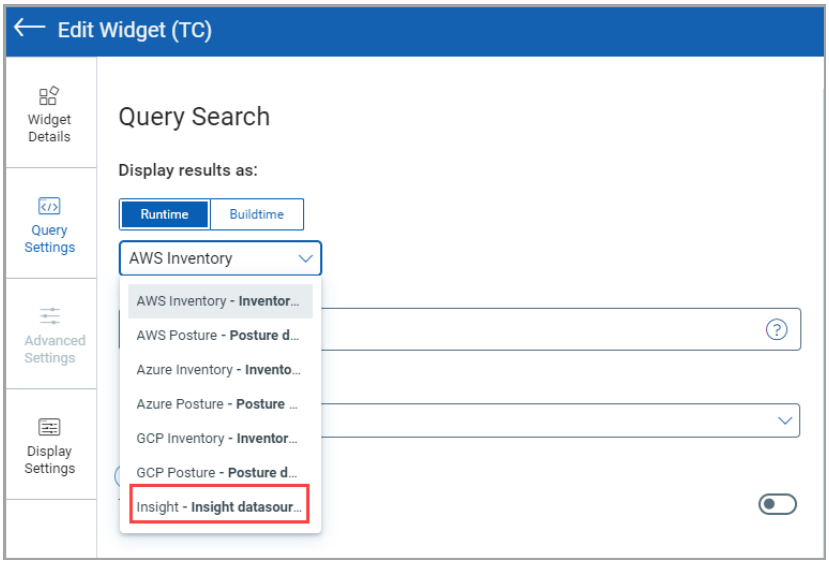
open ports, vulnerable virtual machines, and intrusion attempts across all your accounts.



With the new Insights tab in TotalCloud 2.7, we empower you to take control of your cloud security and make informed decisions to protect your valuable assets.

Note:

-If you already have Insights widgets customized on your dashboard, you must update the data source from 'AWS Inventory' to 'Insights'. You can also re-create the widget, and the insights data source is applied by default.



-All the QQL tokens available for Insights Listing and Insights Detail page apply to the Insights dashboard widget.

New Tokens

With this release, we have introduced support for new tokens.

Insight Listing Tokens

You can find this token for Insights introduced in the new **Insights** tab of TotalCloud. Use these tokens to find insights applicable to the resources specified.

Navigate to **Insights** and search for your required insight.

Name	Description
cloud.id	Find insights belonging to a specified cloud ID.
account.alias	Find connectors based on the account alias associated with the connector/ARN at the time of creation.
connector.name	Find insights associated with the specified connector name.
tags.name	Find the resources with the specified tag you are looking for.
resource.name	Find insights associated with the specified resource name.
resource.id	Find insights associated with the specified resource id.
region	Find insights associated with the specified region.
resource.type	Find resources of speicifed resource type.
service.type	Find insights associated with the specified service type.
riskScore	Find insights associated with the specified risk score.

Insight Details Token

You can find this token for Insights introduced in the new **Insights** tab of TotalCloud. Use these tokens to find insights applicable to the resources specified.

Name	Description
cloud.id	Find insights belonging to a specified cloud ID.
region	Find insights associated with the specified region.
riskScore	Find insights associated with the specified risk score.

Azure Vulnerabilities Tokens

We have introduced a new search query bar under Azure Virtual Machine resources for Vulnerabilities in the Inventory tab of TotalCloud. Use the below token to find vulnerabilities.

Navigate to **Inventory** > **Virtual Machines** > And provide the values under the Virtual Machine or Vulnerabilities search query bar.

Virtual Machine Tokens

You can find this token for virtual machines introduced in the 'Virtual Machines' view under the **Inventory** tab of TotalCloud. Use these tokens to find the virtual machines specified.

Name	Description
virtualmachine.networkInterface.subnetId	Find VMs with a specified network interface address ID.
virtualmachine.networkInterface.privateDnsName	Find VMs having network interface with a specified private DNS name.
virtualmachine.networkInterface.privateIpAddress	Find VMs having network interface with a specified private IP address.
virtualmachine.networkInterface.secondaryPrivateIp	Find VMs having network interfaces with a specified secondary private IP address.
virtualmachine.networkInterface.publicIp	Find VMs having network interfaces with a specified public IP address.
virtualmachine.networkInterface.ipv6Ip	Find VMs having network interfaces with a specified IPv6 IP address.
virtualmachine.isDockerHost	Find VMs that have a docker installed on the host.
virtualmachine.docker.version	Find VMs of the Docker version you are looking for.

Vulnerability Tokens

You can find this token for vulnerabilities introduced in the 'vulnerabilities' view under the **inventory** tab of TotalCloud. Use these tokens to find the vulnerabilities specified.

Name	Description
vulnerability.qid	Find vulnerabilities with the specified QIDs.
vulnerability.severity	Find vulnerabilities with the specified severity.
vulnerability.customerSeverity	Find vulnerabilities with the specified customer severity.
vulnerability.exploitability	Find vulnerabilities the specified exploit description.
vulnerability.patchAvailable	Use the values true | false to find vulnerabilities with patch available.
vulnerability.firstFound	Use a date range or specific date to define when findings were first found.
vulnerability.lastFound	Use a date range or specific date to define when findings were last found.
vulnerability.title	Find vulnerabilities the specified title.
vulnerability.description	Find vulnerabilities the specified vulnerability

	description.
vulnerability.cveIds	Find vulnerabilities with the specified CVE id.
vulnerability.category	Find vulnerabilities with specified category.
vulnerability.cvss3Info.baseScore	Find vulnerabilities with the specified CVSS base score.
vulnerability.cvssInfo.accessVector	Find vulnerabilities based on their access Vector.
vulnerability.cvss3Info.temporalScore	Find vulnerabilities with the CVSS temporal score .
vulnerability.port	Find vulnerabilities with specified open port.
vulnerability.protocol	Find vulnerabilities with the specified protocol
vulnerability.hostOS	Find vulnerabilities with the specified instance operating system.
vulnerability.typeDetected	Find vulnerabilities with the specified detection type.
vulnerability.PCI	Use the values true | false to find vulnerabilities that must be fixed for PCI Compliance (per PCI DSS).
vulnerability.authTypes	Find vulnerabilities with the specified authentication type
vulnerability.bugTraqIds	Find vulnerabilities with the specified Bug Traq ID.
vulnerability.compliance.description	Find vulnerabilities with the specified compliance description.
vulnerability.compliance.section	Find vulnerabilities with the specified compliance section.
vulnerability.compliance.type	Find vulnerabilities with the specified compliance type.
vulnerability.consequence	Find vulnerabilities with the specified conseque
vulnerability.flags	Find the Qualys-defined vulnerability property of interest (e.g. REMOTE, WINDOWS_AUTH, UNIX_AUTH, PCI_RELATED etc).
vulnerability.lists	Find the vulnerability list of interest (e.g. SANS_20, QUALYS_20, QUALYS_INT_10, QUALYS_EXT_10).
vulnerability.patches	Find vulnerabilities with the specified patch QID.
vulnerability.published	Find vulnerabilities with specified date range or dates.
vulnerability.risk	Find the vulnerability based on specified risk.
vulnerability.os	Find vulnerabilities based on the operating system they were detected on.
vulnerability.cvssInfo.baseScore	Find vulnerabilities with the specified CVSS base score.
vulnerability.cvssInfo.temporalScore	Find vulnerabilities with the specified CVSS temporal score .
vulnerability.discoveryTypes	Select a discovery type (Remote or Authenticated) to find instances with vulnerabilities having this discovery type.
vulnerability.sans20Categories	Find vulnerabilities in the SANS 20 category (e.g. Anti-virus Software, Backup Software, etc).
vulnerability.solution	Find vulnerabilities with the specified solution.
vulnerability.status	Find vulnerabilities based on selected status value (ACTIVE, FIXED, NEW, REOPENED)

vulnerability.supportedBy	Select a Qualys service (VM, Agent type, etc) to show vulnerabilities that this service can detect.
vulnerability.vendorRefs	Find the vendor reference .
vulnerability.vendors.productName	Find the vendor product name .
vulnerability.vendors.vendorName	Find the vendor name .
vulnerability.disabled	Use the values true | false to define vulnerabilities that are disabled.

Control Changes

Changes introduced to Controls and Policies in TotalCloud 2.7.0.

Amazon Web Services

Control changes for Amazon Web Services.

New Controls in AWS Infrastructure-as-Code Security Best Practices Policy
We have introduced a new control for AWS Infrastructure-as-Code Security Best Practices Policy.

Platform	CID	Title
AWS	256	Ensure the trail is configured on the organization level.
AWS	413	Ensure that your Amazon Relational Database Service (RDS) instances have the Storage AutoScaling feature enabled.
AWS	435	Ensure the Performance Insights feature is enabled for your Amazon RDS database instances.
AWS	438	Ensure AWS SNS topics do not allow HTTP subscriptions.
AWS	517	Ensure the customer master key (CMK) is not disabled for AWS Key Management Service (KMS).
AWS	531	Ensure that your Amazon Neptune database instances are using KMS Customer Master Keys (CMKs).
AWS	411	Ensure that a log driver has been defined for each active Amazon ECS task definition.
AWS	485	Ensure to enable CloudWatch logging in the audit logging account in the regions.
AWS	489	Ensure multi-az is enabled for AWS DMS instances.
AWS	490	Ensure auto minor version upgrade is enabled for AWS DMS instances.
AWS	505	Ensure that EMR cluster is configured with security configuration.
AWS	506	Ensure AWS Elastic MapReduce (EMR) clusters capture detailed log data to Amazon S3.
AWS	509	Ensure egress filter is set as DROP_ALL for AWS Application Mesh.
AWS	514	Ensure sufficient data retention period is set for AWS Kinesis Streams (7 days or More).
AWS	527	Ensure to encrypt the destination bucket in s3 in the audit logging account in the regions.
AWS	529	Ensure detailed monitoring is enabled for AWS Launch Configuration.
AWS	455	Ensure backtracking is enabled for AWS RDS cluster.
AWS	456	Ensure database retention is set to 7 days or more for AWS RDS cluster.
AWS	457	Ensure Aurora Serverless AutoPause is enabled for RDS cluster.
AWS	458	Ensure connection draining is enabled for AWS ELB.

Platform	CID	Title
AWS	459	Ensure Enhanced VPC routing should be enabled for AWS Redshift Clusters.
AWS	460	Ensure that content encoding is enabled for API Gateway Rest API.
AWS	503	Ensure to configure TLS security policy for the custom domains.
AWS	508	Ensure AWS EBS Volume has a corresponding AWS EBS Snapshot.
AWS	510	Ensure secrets should be auto rotated after not more than 90 days.
AWS	511	Ensure CORS is configured to prevent sharing across all domains for AWS API Gateway V2 API.
AWS	465	Ensure stage caching is enabled for AWS API Gateway Method Settings.
AWS	512	Ensure storage encryption is enabled for AWS Neptune cluster.
AWS	501	Ensure policies are used for AWS CloudFormation Stacks.

Microsoft Azure

Control changes for Microsoft Azure.

New Control in Azure Infrastructure as Code Security Best Practices Policy
We have introduced new controls in Azure Infrastructure as Code Security Best Practices Policy.

Platform	CID	Title
Azure	50391	Ensure that Azure Search Service instances are configured to use system-assigned managed identities.

New Controls in Microsoft Azure Best Practices Policy
We have introduced new controls in Microsoft Azure Best Practices Policy.

Platform	CID	Title	Service	Resource
AZURE	50083	Ensure that Microsoft Defender for SQL is set to ON for critical SQL Servers.	AZURE_SQL	SQL_SERVER
AZURE	50172	Ensure that Azure Defender is set to On for Open-Source Relational Databases.	SECURITY_ CENTER	SECURITY_POLICY
AZURE	50313	Ensure that Azure Storage Accounts are configured with private endpoints.	STORAGE_ ACCOUNT	STORAGE_ACCOUNT
AZURE	50360	Ensure that Azure Defender is set to On for Azure Cosmos DB.	SECURITY_ CENTER	SECURITY_POLICY
AZURE	50458	Ensure that 'cross-tenant replication' is set to disabled.	STORAGE_ACCOUNT	STORAGE_ACCOUNT
AZURE	50457	Ensure that Linux and Windows Disk encryption should be applied on virtual machines is set to On.	SECURITY_CENTER	SECURITY_POLICY

Issues Addressed

- We have enhanced the Public API for control evaluations by including time and date parameters for fetching evaluations. By aligning the criteria in the Public API with the UI, records are now consistently fetched based on date and time, ensuring a coherent representation of the data across both interfaces.
- We have fixed a false positive issue for control ID 50054.
- We have limited API calls for control evaluation to users with the TotalCloud Free license type. This measure prevents unnecessary API calls from Qualys to your Cloud account. Importantly, these restrictions have no impact on the data collection within the inventory of TotalCloud Free users.
- We have introduced pagination support for Elastic Load Balancers, ensuring the discovery of all ELB resources in the TotalCloud inventory.