Tencent Smart Advisor

Product Introduction

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Product Introduction

Overview

Last updated：2022-11-07 11:20:44

Tencent Smart Advisor is an out-of-the-box product that assesses risks for Tencent Cloud resources. After Tencent Smart Advisor is granted to a CAM service role, it can quickly assess and analyze risks in cloud resources, application architecture, business performance, and security and then offer optimization suggestions online according to the actual business usage, helping improve the system security, business stability, and service reliability.

List of supported products

Tencent Smart Advisor provides a wide variety of assessment items, flexible assessment configurations, and system optimization suggestions to help you improve business continuity.

It offers various risk assessment items in multiple dimensions, such as security, reliability, cost, service restriction, and performance for different Tencent Cloud products. Currently, it can conduct assessment in the following Tencent Cloud products:

Product Name
Cloud Access Management (CAM)
Cloud Block Storage (CBS)
Cloud Connect Network (CCN)
Content Delivery Network (CDN)
Cloud Firewall (CFW)
Message Queue CKafka (CKafka)
Cloud Load Balancer (CLB)
Cloud Object Storage (COS)
Cloud Virtual Machine (CVM)
Cloud Workload Protection (CWP)
TDSQL-C for MySQL (TDSQL-C)
Anti-DDoS

TDSQL for MySQL
DNSPod
Domains
Elastic IP (EIP)
Elasticsearch Service
Cloud Streaming Services (CSS)
TencentDB for MongoDB
TencentDB for MySQL
NAT Gateway
TencentDB for Redis
Security Groups
Tencent Distributed Message Queue (TDMQ)
TencentDB for MariaDB
Tencent Kubernetes Engine (TKE)
Tencent Real-Time Communication (TRTC)
Virtual Private Cloud (VPC)
VPN Tunnels for VPCs
VPN Gateways for VPCs

More Tencent Cloud products and services will be supported, and more risk assessment items will be available.

Features

Last updated：2022-11-07 11:20:44

Tencent Smart Advisor inspection items cover five dimensions: security, reliability, service restriction, cost, and performance.

Security

We recommend you enable the Tencent Cloud security features and inspection permissions to improve the system and business security.

Service	Inspection Item	Description
Network ACL	Public network access permissions	Check whether the network ACL policies allow for source IP access through all ports or ports except 80 and 443, and if so, security risks such as unauthorized access and DDoS attacks will occur.
CAM	Account-MFA device binding	Check whether an account is bound to an MFA device, and if not, dynamic verification code-based MFA is not required for account login, reducing the security level.
	Account protection enablement	Check whether features such as login protection, sensitive operation protection, and remote login protection are enabled, and if not, MFA is not required for corresponding operations, reducing the security level.
CDN	IP access frequency limit	If this feature is not enabled, the number of access requests per second from one single IP/node cannot be limited, making the server vulnerable to high-frequency CC attacks and hotlinking by malicious users.
CFW	Resource protection	Check the CFW protection policy. If it is not enabled for CVM, NAT, VPN, or CLB instances, a risk warning will be triggered.
CLB	Expiration of certificates bound to instances	Check whether the certificates bound to CLB instances have expired.
COS	Sub-account access permission not restricted	Check the sub-account permission scope of COS buckets. If a sub-account has full access to buckets, the buckets might have security risks.
	Public read/write	Check the public read/write permissions of COS buckets. If such permissions are set, anonymous user groups can directly read from and write to the

	permissions of buckets	corresponding buckets, which brings high security risks. We recommend you not grant such permissions in buckets.
	CORS configuration of buckets	Check the CORS configuration of buckets. If a CORS rule exists but the "Allow-Headers" or "Expose-Headers" header of CORS is not configured, cross-origin access requests might fail.
	Referer hotlink protection configuration of buckets	Check the permission and referer configurations of COS buckets. If the bucket permission allows access by anonymous users, but no referer access rule is configured or an empty rule is configured, problems such as hotlinking by malicious users might occur.
CWP	Vulnerabilities not fixed	Check whether an instance has unfixed vulnerabilities, and if so, an instance might be compromised and data loss might be occurred.
	Client offline	Check whether the CWP client is offline, and if so, the CWP instance will not be able to protect your instance.
TDSQL-C	TDSQL-C for MySQL root account security	Check the account configuration. If only the root account exists and there are no other application accounts, the permissions are excessive, and data security risks due to faulty or malicious operations will occur.
Anti-DDoS	Available IP blackhole unblockings	Check whether the proportion of used blackhole unblockings is excessive.
	Blocked EIPs	Check whether there are any EIPs blocked due to DDoS attacks.
TDSQL for MySQL	Restriction of high-risk commands for accounts	Check the account configuration. If all accounts have the permission to run global commands, such as DROP and DELETE, data may be easily deleted by mistake or maliciously.
	Public network security policy	Check the public network security policy. If public network access is enabled, but no security group rules are configured, when there are attacks from the public network, application exceptions and data breach will occur.
ES	Public network access policy of ES clusters	Check the public network access policy of ES clusters. If no restrictions are configured, a warning for access risk in the cluster will be triggered, and the bandwidth for public network access will be limited.
	Kibana component's public network access policy of clusters	Check the Kibana component's public network access policy of ES clusters. If no restrictions are configured, a warning for access risk in Kibana will be triggered.

TencentDB for MySQL	Root account security	Check TencentDB for MySQL account configuration. If only the root account exists and there are no other application accounts, the permissions are excessive, and data security risks due to faulty or malicious operations will occur.
	Restriction of high-risk commands for non-root accounts	Check the permission scope of TencentDB for MySQL non-root accounts. If an application account has the permission to run high-risk commands, such as DROP and DELETE, data may be easily deleted by mistake or maliciously.
	Public network security policy	Check the public network security policy in TencentDB for MySQL. If public network access is enabled, but no security group rules are configured, when there are attacks from the public network, application exceptions and data breach might occur.
TencentDB for Redis	High-risk commands	Check the disabled command configuration of TencentDB for Redis instances. If a high-risk command is not disabled, risks such as application blocking and accidental data deletion will occur.
Security Group	Public network access	Check whether the security group allows for source IP access through all ports or ports except 80 and 443, and if so, security risks such as unauthorized access and DDoS attacks will occur.
TencentDB for MariaDB	Restriction of high-risk commands for accounts	Check the account configuration. If all accounts have the permission to run global commands, such as DROP and DELETE, data might be easily deleted by mistake or maliciously.
	Public network security policy	Check the public network security policy. If public network access is enabled, but no security group rules are configured, when there are attacks from the public network, application exceptions and data breach might occur.

Reliability

Multidimensional monitoring is supported to keep instances running stably.

Service	Inspection Item	Description
CBS	Storage capacity	Check the storage capacity usage of CBS cloud disks. If the capacity utilization is excessive, cloud disk read/write will be affected.

	No snapshots created	Check whether CBS cloud disks have snapshots or are configured with a scheduled snapshot policy, and if not, it will be difficult to recover the data when a server or cloud disk is faulty, which may cause serious data loss.
CKafka	Cross-AZ deployment	If instances are not deployed across AZs, when a serious fault occurs in the single-AZ CKafka cluster, the cluster may become unavailable.
CLB	CVM instance AZ	Check whether a CLB instance is in the same AZ as the CVM instance bound to it, and if not, cross-AZ forwarding may affect service reliability, for example, slower forwarding of some requests.
	Single points of failure of the real server	Check whether a CLB listener or forwarding rule is bound to only one real server, such as CVM or EVM instance, and if so, single points of failure may occur.
	Forwarding rule bound to multiple ports of a CVM instance	Check whether a CLB forwarding rule is bound to multiple ports of the same CVM instance, and if so, it will be harder to troubleshoot problems when processes compete for resources as the business volume grows, and the system will be less able to accommodate traffic peaks.
	CVM instances in different subnets	Check whether a CLB listener or forwarding rule is bound to multiple CVM instances in different VPC subnets, and if so, it will be harder to quickly troubleshoot problems when exceptions occur.
	CVM instance weight	Check the weight of the CVM instance bound to a CLB listener or forwarding rule. If the weight doesn't match the configuration, performance risks will occur during business peaks, affecting business stability.
	Health check configuration	Check whether health check is configured for a CLB instance, and if not, the CLB instance will forward traffic to all real servers (including abnormal ones).
	Forwarding rule configuration	Check the CLB listener configuration. If no forwarding rules are configured, CLB features cannot be used normally, and additional fees will be incurred.
	Sudden changes in the health check	Check for sudden changes of CLB listeners in the health check, i.e., whether the server port is abnormal.
	Instance type	Check the CLB instance type, which is either classic or application. Application instances have more features, for example, layer-4 listener that can be configured with different real servers, layer-7 listener, CLS log, SNI, and binding with ENI.

	Bandwidth cap of 1 Mbps	If the bandwidth is not selected during CLB instance purchase, the default limit of 1 Mbps will apply. CLB instances with this limit are scanned, and if they are used by high-traffic businesses, serious packet loss may occur.
COS	Bucket versioning	Check the versioning configuration of COS buckets. If it is not enabled, data may be lost.
	Log management configuration of buckets	Check the log management feature of COS buckets. If the owners of the destination and source buckets are different, bucket log shipping will fail.
CVM	System disk snapshot	Check CVM system disk snapshots. If no snapshots are created, it will be difficult to recover the data when a server or cloud disk is faulty, which may cause serious loss.
	Excessive disk utilization of instances	Check the disk utilization of CVM instances. If the utilization is excessive, disk read/write will be affected.
	Local disk type of instances	Check the local disk usage of CVM instances. If an instance is not an I/O or Big Data model but uses a local disk, its disk data cannot be backed up through snapshots, which may bring risks to disaster recovery.
	Excessive bandwidth utilization	Check the bandwidth utilization of CVM instances. If the utilization is excessive, the network performance may be affected.
Anti-DDoS	Layer-7 forwarding rule health check	Check whether any exceptions exist in the health check of the current layer-7 forwarding rules.
TDSQL for MySQL	Disaster recovery	Check whether disaster recovery is configured for instances, and if not, business access may be affected when an instance has a serious fault.
EIP	Bandwidth cap of 1 Mbps	If the EIP bandwidth is not selected during purchase, the default limit of 1 Mbps will apply. EIPs with this limit are scanned, and if they are used by high-traffic businesses, serious packet loss may occur.
ES	Automatic snapshot backup of ES clusters	Check the automatic snapshot backup of ES clusters. If it is not configured, a risk warning will be triggered.
CSS	CSS code mode	Check whether the service is in CSS code mode, and if not, a risk warning will be triggered.

	Resolution of CNAME record to dedicated domain name	If the CNAME record of the domain name is incorrectly configured, normal push and playback in CSS will be affected. If the CNAME record value is incorrect, a risk warning will be triggered.
	Top-level/Second-level domain names included in push domain name	A second-level domain name is a subordinate of a top-level domain name. CSS domain names are redirected to wildcard domain names through CNAME records, and the domain names will be instantiated if necessary. If a top-level domain name is instantiated, but its second-level domain names are not, normal resolution of the second-level domain names will be affected.
	Top-level/Second-level domain names included in playback domain name	A second-level domain name is a subordinate of a top-level domain name. CSS domain names are redirected to wildcard domain names through CNAME records, and the domain names will be instantiated if necessary. If a top-level domain name is instantiated, but its second-level domain names are not, normal resolution of the second-level domain names will be affected.
	Push authentication enablement	Check whether push authentication is enabled and CSS callback is configured, and if both are not, a risk warning will be triggered.
	SSL certificate validity period	If the certificate expires, HTTPS access will be affected, i.e., HTTPS access requests may fail.
	Bandwidth cap value	Check whether the bandwidth cap is enabled, and if so, check whether the current bandwidth is close to the cap. After the cap is reached, new user access requests will be limited.
TencentDB for MongoDB	Oplog retention period	Check the oplog retention period of TencentDB for MongoDB instances. If the period is too short, it may cause rollback failures or affect troubleshooting.
	Backup result	Check whether TencentDB for MongoDB instances are successfully backed up, and if not, data may fail to be recovered.
	Classic network	Check whether TencentDB for MongoDB instances use classic networks.
TencentDB for MySQL	Disaster recovery	Check whether disaster recovery is configured for TencentDB for MySQL instances, and if not, business access may be affected when an instance has a serious fault.

	Source-replica delay	Check the source-replica delay of TencentDB for MySQL instances. If the delay is excessive, risks such as removal of database RO instances and excessive source/replica HA switch time will occur.
	Cross-AZ deployment	Check whether TencentDB for MySQL instances are deployed across AZs, and if not, when a severe fault occurs in the AZ, access to the database may fail.
	Single instance in a read-only group	Check whether a TencentDB for MySQL read-only group has only one instance, and if so, the read-only business will become unavailable when the instance fails.
	Classic network	Check whether TencentDB for MySQL instances use classic networks.
TencentDB for Redis	Cross-AZ deployment	Check whether TencentDB for Redis instances are deployed across AZs, and if not, when an AZ-level disaster occurs in an instance, it may become inaccessible.
	Classic network	Check whether TencentDB for Redis instances use classic networks.
Security Group	Redundant rules	Check for ineffective security group rules, which occupy the limited quota and may result in the failure to create rules and affect your business. Ineffective rules can be repeated and involve port overlaps.
TDMQ	Cluster health check	Use of unhealthy clusters may involve certain risks.
	Backup consumer	Check whether there is only one consumer, and if so, when a single point of failure occurs, business consumption will be affected.
	Dead letter queue	If there are no dead letter queues, consumers may be unable to process some special messages.
TencentDB for MariaDB	Source-replica delay	If the source-replica delay is continuously excessive, source-replica data consistency cannot be guaranteed. In this case, if an HA source-replica switch occurs on an instance, data may be lost in extreme cases.
	Disaster recovery	Check whether disaster recovery is configured for TencentDB for MariaDB instances, and if not, business access may be affected when an instance has a serious fault.
TKE	Cross-AZ cluster node deployment	Check whether the cluster nodes are in the same AZ, and if so, when the AZ is unavailable, the business will be affected, and the cluster cannot be scheduled to other AZs.

TRTC	Terminal version of the native SDK	Check the native SDK terminal version. If it is earlier than expected, the quality may be unstable.
	Terminal version of the web SDK	Check the web SDK terminal version. If it is earlier than expected, the quality may be unstable.
	Video bitrate of the native SDK	Check the video bitrate of the native SDK. Video parameters need to balance image quality and smoothness. Configuring reasonable video parameters will deliver a better user experience.
	Scenario consistency of the native SDK	Check whether the same room involves multiple call scenarios, and if so, unexpected results may occur.
	Time sequence for stream pull of the native SDK	Check the time sequence for stream pull of the native SDK. If a pull operation is earlier than the arrival of the video stream, the screen may turn black.
	Logic for room exit of the native SDK	Check the logic for room exit of the native SDK. If it is not properly configured, the SDK will experience internal chaos with exceptions.
	Postpaid billing	Check whether postpaid billing is enabled, and if not, the service will be suspended after the plan is used up.
	Substream video bitrate of the native SDK	Check the substream video bitrate of the native SDK. Video parameters need to balance image quality and smoothness. If the bitrate is low, poor image quality or video lag may be caused under poor network conditions.
	Room entry scenario and role match in the native SDK	Check whether the scenario matches the role configuration in the native SDK. For example, in video and audio call scenarios, the audience role doesn't need to be set; otherwise, a lag or black screen may occur.
	Mutual kick-out under the same `userId` in the native SDK	Check for mutual kick-out in the same room under the same `userId` in the native SDK. This problem may lead to a black screen or lag.

VPC	Subnet planning	Check whether the subnet IP range is identical to the VPC IP range, and if so, no more subnets can be planned, adversely affecting long-term plans such as cross-AZ expansion.
VPC - VPN Gateway	Expiration in one month	Check the billing mode of VPN gateways. If manual renewal or non-renewal is enabled and a VPN gateway will expire soon, the service may become unavailable, affecting the business.
VPC - VPN	VPN tunnel status	Check whether there is a VPN tunnel that is not connected, and if so, switching to the secondary tunnel may fail.

Service Restriction

Tencent Smart Advisor can monitor the maximum number of available service resources to prompt you to delete resources or apply to increase the quota based on the suggestions.

Service	Inspection Item	Description
CFW	Rule quota	Check the CFW rule list quota. If it is insufficient, a risk warning will be triggered.
CVM	Instance expiration	Check whether CVM instances have expired. If a monthly subscribed instance is about to expire but auto-renewal is not configured, it may be terminated after expiration.
TDSQL-C	TDSQL-C for MySQL cluster expiration	Check whether clusters have expired. If a monthly subscribed cluster is about to expire but auto-renewal is not configured, access to the business may be compromised after expiration.
TDSQL for MySQL	Instance expiration	Check whether instances have expired. If a monthly subscribed instance is about to expire but auto-renewal is not configured, access to the business may be compromised after expiration.
DNSPod	Paid plan expiration in two months and auto-renewal not configured	Check whether a paid plan will expire in two months and auto-renewal is configured. If it is not configured, the service will be suspended immediately the plan is used up.
Domain	Expiration	Check whether domain names have expired. If auto-renewal is not configured, access to the business may be compromised after expiration.
EIP	Usage	Check the usage of EIPs in each region. If the usage is close to or

		exceeds the quota, no more EIPs can be applied for.
TencentDB for MongoDB	Instance expiration	Check whether TencentDB for MongoDB instances have expired. If a monthly subscribed instance is about to expire but auto-renewal is not configured, access to the business may be compromised after expiration.
	Storage capacity	Check the storage capacity utilization of TencentDB for MongoDB instances. If the utilization reaches 100%, write will fail.
TencentDB for MySQL	Instance expiration	Check whether TencentDB for MySQL instances have expired. If a monthly subscribed instance is about to expire but auto-renewal is not configured, access to the business may be compromised after expiration.
	Connection utilization	Check the connection utilization of TencentDB for MySQL instances. If the utilization reaches 100%, the business may fail to connect to the database.
	Disk utilization	Check the disk utilization of TencentDB for MySQL instances. If the utilization is excessive, data may fail to be written.
	Disk usage close to the upper limit of 6 TB	Check whether the disk usage of TencentDB for MySQL instances is close to the upper limit of 6 TB.
NAT Gateway	DNAT usage	Check the DNAT usage of NAT gateways. If the usage is close to the upper limit, further business deployment may be affected.
TencentDB for Redis	Instance expiration	Check whether TencentDB for Redis instances have expired. If a monthly subscribed instance is about to expire but auto-renewal is not configured, access may fail.
	Memory close to the upper limit of 4 TB	Check whether the memory usage of TencentDB for Redis instances is close to the upper limit of 4 TB.
	Number of replicas reaching the upper limit of five	Check whether the number of TencentDB for Redis instance replicas reaches the upper limit of five.
TencentDB for MariaDB	Connection utilization	If the connection utilization reaches 100%, new requests cannot establish connections, and access will fail.
	Data disk utilization	If the disk utilization reaches 100%, write will fail.
	Instance expiration	Check whether TencentDB for MariaDB instances have expired. If a monthly subscribed instance is about to expire but auto-renewal is not

		configured, access to the business may be compromised after expiration.
VPC	Number of used route tables	Check the number of VPC route tables. If it is close to or exceeds the upper limit, new tables may fail to be created.

Cost

Tencent Smart Advisor can provide suggestions for more cost-effective configurations based on the running status of resources to reduce your costs.

Service	Inspection Item	Description
CBS	Underutilization	Check the mounting and I/O status of CBS cloud disks. If a cloud disk was unmounted in the past five days, or its daily IOPS did not exceed one in the last seven days, an alarm will be triggered. Cloud disks that are idle for a long time will incur unnecessary fees.
CLB	Idle instances	Check whether CLB instances are bound to backend Tencent Cloud resources (CVM instances or ENIs), and if not, they will be considered idle, and additional fees will be incurred.
	Low utilization	Check the utilization of CLB instances. If the number of connections is smaller than 10% of the quota, the costs of redundancy may be incurred.
COS	Bucket lifecycle configuration	Check whether the lifecycle rules of COS buckets are configured, and if not, objects that are accessed infrequently in buckets will incur unnecessary fees.
	Incomplete multipart uploads in buckets	Check for the incomplete multipart upload clearing rules of COS buckets. If no such rules are configured, unnecessary fees may be incurred.
CVM	Low utilization of instances	Check the CPU and network I/O utilization of CVM instances. If it is low for a long time, a risk warning will be triggered.
	Billing mode	Check whether CVM instances are in pay-as-you-go billing mode for a long time (more than two months). The unit price in this mode is high, which will incur unnecessary fees.
TDSQL-C	DSQL-C for MySQL underutilization	Check whether clusters are idle. If the business lifecycle is stable, resources that are idle for a long time will incur unnecessary fees.

TencentDB for MongoDB	Underutilization	Check whether instances are idle. If the business lifecycle is stable, resources that are idle for a long time will incur unnecessary fees.
TencentDB for MySQL	Underutilization	Check whether instances are idle. If the business lifecycle is stable, resources that are idle for a long time will incur unnecessary fees.
NAT Gateway	Idleness	Check whether NAT instances are configured in route tables, and if not, they will be idle and incur fees.
TencentDB for Redis	Underutilization	Check whether instances are idle. If the business lifecycle is stable, resources that are idle for a long time will incur unnecessary fees.
TencentDB for MariaDB	Underutilization	Check whether instances are idle. If the business lifecycle is stable, resources that are idle for a long time will incur unnecessary fees.
VPC - VPN Gateway	Idleness	Check whether VPN gateways are associated with VPN tunnels, and if not, additional fees may be incurred.

Performance

Tencent Smart Advisor provides performance improvement suggestions based on the resource usage monitored during instance operations and best practices.

Service	Inspection Item	Description
CBS	High I/O load	Check the I/O load of CBS cloud disks. If it is excessive, an alarm will be triggered.
	Excessive IOPS	Check whether the peak IOPS of CBS cloud disks reaches the upper limit configured for the corresponding cloud disk type, and if so, traffic throttling may be triggered.
	Excessive throughput	Check whether the peak throughput of CBS cloud disks reaches the upper limit configured for the corresponding cloud disk type, and if so, traffic throttling may be triggered.
CCN	Outbound bandwidth usage	Check whether the outbound bandwidth usage of cross-region CCN instances in each region is close to the threshold, and if so, packets may be lost due to bandwidth limiting, affecting the business.

CDN	Single-link downstream speed limit configuration	If this feature is not set, the single-link speed is not limited by default, which may cause a high peak bandwidth during events.
	Bandwidth cap configuration	If this feature is not disabled, when the bandwidth cap is reached, the CDN service will be disabled, and requests will be forwarded to the origin server or the 404 error code will be returned. This feature can reduce bandwidth fees to a certain degree. After the CDN service is disabled, you need to set and enable the domain name again before you can use the CDN service again.
	Expiration of certificates bound to domain names	If the certificate expires, HTTPS access will be affected, i.e., HTTPS access requests may fail.
	Cache hit rate	If the hit rate is low, the pressure on the origin server cannot be effectively alleviated, and user access acceleration cannot reach a satisfactory optimization effect.
	Error code proportion	If the proportion of error codes is high, events affecting the business may have occurred, or there will be potential faults.
	Secondary origin server	If no secondary origin servers are configured, when the primary origin server is unavailable, disaster recovery will be impossible.
CLB	404 or 502 error code returned by the real server	Check whether the CLB real server returns the 404 or 502 error code, which indicates that no corresponding resources can be found or a gateway error occurs, and if so, business quality may be affected.
COS	5xx error rate	Check COS error codes. If there are too many 5xx error codes with a high occurrence frequency, normal access to buckets may be affected.
CVM	High memory load of instances	Check the memory utilization of CVM instances. If it is excessive, a risk warning will be triggered.
	High CPU load of instances	Check the CPU utilization of CVM instances. If it is excessive, a risk warning will be triggered.
TDSQL-C	TDSQL-C for MySQL	Check the CPU utilization. If it is excessive, risks such as longer business request delays and no response will occur.

	CPU utilization	
	TDSQL-C for MySQL number of full-table scans	Check the number of full-table scans of instances per second.
TencentDB for MongoDB	Dirty data in cache	Check the dirty data in the cache of TencentDB for MongoDB instances. If its proportion exceeds 20%, user threads will be flushed, and the business will be blocked.
	CPU utilization	Check the CPU utilization of TencentDB for MongoDB instances. If it is excessive, risks such as longer business request delays and waits will occur.
TencentDB for MySQL	CPU utilization	Check the CPU utilization of TencentDB for MySQL instances. If it is excessive, risks such as longer business request delays and no response will occur.
	Number of running threads	Check the number of running threads on TencentDB for MySQL instances. If it is far more than the number of CPU cores, risks such as longer request waits and delays will occur.
TencentDB for Redis	Outbound traffic throttling triggered on proxy nodes	Check the number of trigger times of outbound traffic throttling on TencentDB for Redis proxy nodes. If traffic throttling was triggered, the business may have been compromised during peak hours. If the number is excessive, business traffic has reached the upper limit, and business access may have longer delays or fail.
	CPU utilization	Check the CPU utilization of TencentDB for Redis instances. If it is excessive for a long time, problems such as longer request delays and request blocking may occur.
	Excessive node requests	Check whether the number of requests of TencentDB for Redis nodes is close to the upper limit.
TencentDB for MariaDB	CPU utilization	If the CPU utilization is high, the current instance is busy, and problems such as slower and blocked queries may occur.
	Number of active connections	If the number of active connections is excessive, the instance is currently under high pressure, and requests are likely to be blocked.

Strengths

Last updated：2022-11-07 11:20:44

Diverse assessment items

Tencent Smart Advisor offers various assessment items in multiple dimensions, such as security, reliability, cost, service restriction, and performance for different Tencent Cloud products. More Tencent Cloud products and services are to be supported.

Flexible assessment configurations

You can add or delete assessment items, or ignore the items that you are not concerned to get neat assessment reports and focus on the key metrics.

You can ignore specific cloud resources to focus on assessing the execution status of key resources.

Systematic optimization suggestions

Based on the best practices accumulated over Tencent Cloud's many years of customer service, Tencent Smart Advisor provides systematic, targeted, and practical optimization suggestions for each assessment item to help you take preventive measures and improve business continuity.

Use Cases

Last updated：2022-11-07 11:20:44

Daily Ops

Tencent Smart Advisor can regularly assess the health of cloud resources, rate the risks of cloud architectures and resources, and offer optimization suggestions online to help you improve business continuity.

Promotional events support

Service usage can be assessed in advance to check the stress level of your Tencent Cloud resources, so you can submit a ticket as needed to add more resources based on the estimated promotion scale and ensure the smooth operation of the event.

Proactive architecture optimization

Tencent Smart Advisor can verify the security, fault tolerance, and backup capabilities of architectures to ensure the continuous and stable operation of businesses. You can actively trigger inspections as needed.