Alibaba Cloud Threat Detection

Product Introduction

Issue: 20181211

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade

secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 What is Threat Detection Service (TDS)?

Alibaba Cloud Security offers Threat Detection Service (TDS) to secure and monitor diagnostics services. TDS supports multiple features, including security event detection, vulnerability scanning, and configuration baseline check. You can use TDS to secure and manage your assets on the cloud. With the integration of Alibaba's independently developed big data and machine learning algorithm, TDS can help you check and process all the security threats in real time.

TDS also enables you to analyze the security situation and detect potential threats by collecting and auditing up to 10 types of security logs, your asset fingerprints, and network threat intelligence.

Features of TDS

TDS supports the following features:

- **Security events**: TDS detects network intrusions and generates alarms in real time. For example, TDS can detect unusual logons, webshell injections, unusual server activities, and virus attack.
- **Vulnerability scanning**: TDS automatically scans vulnerabilities on the servers and provides vulnerability fixes. It can also detects and fix web content management system (WCMS) vulnerabilities, Linux vulnerabilities, and Windows vulnerabilities.
- **Baseline check**: TDS periodically checks the server configuration using either the default or customized scan policies. The baseline check includes security compliance check, system configuration check, account check, and weak password check.
- **Asset fingerprints**: Collects and records asset running information, including processes, system accounts, open ports, software versions, and website background information.
- **Log retrieval**: TDS provides an all-in-one log retrieval service for you to query and manage up to 10 types of server and web logs so that you can track the causes of security issues.

2 Features

Threat Detection Service (TDS) is available with the Basic Edition and the Enterprise Edition:

- Basic Edition: Detects unusual logon and server vulnerabilities for free.
- Enterprise Edition: supports annual and monthly subscriptions, and provides comprehens ive security services, such as security events, server vulnerability detection and resolution, baseline check, asset fingerprints, and log retrieval.

For more information about the features of the Basic Edition and Enterprise Edition, see the following:

Comparison of features between the Basic Edition and the Enterprise Edition

The following table lists the features of TDS and compares the differences between the Basic Edition and the Enterprise Edition:

- ×: indicates that the related feature is excluded in the service.
- √: indicates that the related feature is included in the service.
- Value-added: indicates that you must select the related feature to include it in your purchase.

Feature	Item	Description	Basic Edition	Enterprise Edition
Security events	Unusual logon detection	Basic • Logon from unusual locations: TDS automatically records locations that are commonly used to log on to Elastic Compute Service (ECS) instances. You can also manually specify these locations. The system generates an alarm when a logon from an unusual location is detected. • Brute-force password cracking: detects a logon to ECS instances after multiple failed attempts, which may be caused by brute-force password cracking.	√	√
		Advanced • Invalid IP logon: This feature allows you to specify valid IP addresses to be used to log on to ECS instances, such as bastion host IP addresses and local area network (LAN) IP addresses. Therefore, this system generates an alarm when detecting a logon with an unspecified IP address.	×	√

		• Invalid account logon: This feature allows you to specify the valid accounts for logging on to ECS instances. Therefore, this system generates an alarm when detecting a logon with an unspecified account. • Logon during invalid periods: This feature allows you to specify valid periods, such as office hours, for logging on to ECS instances. Therefore, this system generates an alarm when detecting a logon that does not occur during the specified period.		
Security events	Webshell removal	Webshell detection: checks both instances and networks for web scripts, such as PHP, ASP, and JSP files. • Instance check: monitors the changes of Web directories on an instance in real time. • Network check: simulates Webshell execution and analyzes network protocols.	√ (Checks instances only.)	√
		Webshell removal: easily quarantines the detected Webshell in the console. You can restore the Webshell within 30 days after isolation.	×	√
Security events	Malicious processes (malware checking)	Virus detection: Periodically scans processes, monitors process initiation events, and detects malicious viruses and Trojans using the anti-virus mechanism in the cloud. Virus removal: easily terminates processes and quarantines malicious files in the console. Scope of virus targets: • Ransomware: file-encrypting ransomware such as WannaCry and CryptoLocker. • Malicious attacks: Distributed Denial-of-Service (DDoS) Trojans, malicious scanning Trojans, and spam Trojans. • Mining software: resource consumption software that uses instances for illegal virtual currency mining. • Zombies: central control Trojans, malicious central control connections, and hacking tools. • Other viruses: worms, Mirai, and infectious viruses. Virus database: • Update mechanism: updates the virus management in the cloud, and does not provide any on-premises detection engine. • Virus sample coverage: detects all types of viruses, and integrates the worldwide major anti-virus engines	×	√

		, proprietary sandbox, and machine learning engine in the cloud.		
Security events	Suspicious processes	Suspicious process detection: restores intrusion links based on real attack-defense scenarios in the cloud, creates a process whitelist, and generates alarms when detecting illegal and intrusive processes. Scope of suspicious processes: • Reverse shell: suspicious commands in Bash processes, and arbitrary commands remotely executed by instances. • Suspicious database commands: suspicious commands in databases, such as MySQL, PostgreSQL, SQLServer, Redis, and Oracle. • Illegal operations in application processes: illegal operations in application processes, such as Java, FTP, Tomcat, Docker containers, and Lsass.exe. • Illegal system processes: PowerShell, Secure Shell (SSH), Remote Desktop Protocol (RDP), smbd, and secure copy protocol (SCP). • Other suspicious processes: Visual Basic Script (VBScript) execution, accessing instances, writing crontab files, and Webshell injection. Suspicious process coverage: builds more than 1, 000 process patterns for hundreds of processes, and analyzes suspicious processes by comparing them with these patterns.	×	√
Security events	Sensitive file tampering	Tampering detection: monitors sensitive directories and files in real time, and generates alarms when detecting suspicious reading, writing, and deletion processes. Scope of tampering detection: • System file tampering: malicious replacement of processes that run Bash and ps commands, and operation of hidden illegal processes. • Core dump removal: malicious removal of website core dump files after an illegal logon to instances. • Drive-by downloading: malicious code injection into a Web page that causes the auto downloading of Trojans. • Other suspicious events: ransomware on the logon pages of Linux and MysqlDB, creating emails or Bitcoin wallet addresses.	×	√

Security events	Unusual network connection	Unusual connection: monitors connections between instances and networks, and generates an alarm when detecting an illegal connection. Scope of unusual connections: • Active connections to unknown servers: active connections to suspicious IP addresses using reverse shell and Bash commands. • Malicious attacks: malicious software injection used to launch malicious attacks, such as SYN floods, User Datagram Protocol (UDP) floods, and Internet Control Message Protocol (ICMP) floods. • Suspicious communications: suspicious Webshell communications.	×	√
Vulnerability management	Vulnerabilities of Linux software	Detection of Linux software vulnerabilities: compares software versions by using the Open Vulnerability and Assessment Language (OVAL®) matching engine, and generates alarms when detecting vulnerabilities from the Common Vulnerabilities and Exposures (CVE®) vulnerability database.	√	√
		Vulnerability fix: fixes vulnerabilities automatically with easily applied updates, and generates vulnerability fix instructions for manual fixes.	×	√
Vulnerability management	Windows vulnerabilities	Detection of Windows vulnerabilities: obtains updates from Microsoft Updates for the Windows operating system, detects critical and other vulnerabilities, and generates alarms of these vulnerabilities.	√	√
		Vulnerability fix: easily downloads updates, installs the updates silently, and then prompts you to restart the system if a restart is required.	√	√
Vulnerability management	WCMS vulnerabilities	Detection of Web content management system (WCMS) vulnerabilities: monitors Web directories, recognizes common website builders, and checks the vulnerability database to identify vulnerabilities in the website builders.	√	√
		Vulnerability fix: uses proprietary updates developed by Alibaba Cloud to replace or modify source code and allows you to easily fix vulnerabilities.	×	√
Baseline check	Server baseline	Server baseline check: initiates tasks to scan security configurations of servers, and generates notifications of vulnerable configurations.	×	√

		Scope of server baseline check: • Account security: password policy compliance, and weak passwords of systems and applications. • System configurations: potential risks in group policies , logon baseline policies, and registry configurations. • Databases: critical threats in the configurations of databases such as Redis. • Compliance requirements: compliance with system baseline requirements, such as the CIS-Linux Centos7 benchmark. Check policy: supports a customized check policy that specifies the checked items, check cycle, and target server group. The system does not support customized check scripts.		
Asset fingerprints	Asset fingerprints	Port: collects and displays port listening information, and records changes to track opened ports. Account: collects information about accounts and related permissions, and checks privileged accounts for privilege elevation. Process: collects and displays process snapshots to track normal processes and detect unusual processes. Software: checks software installation information, and in the case of critical vulnerabilities, quickly locates affected assets. Website background: recognizes website back-end assets, and detects user enumeration attempts and unusual background logons.	×	√
Log retrieval	Log retrieval	Server logs • Logon: searches logs of SSH and RDP logon processes. • Brute-force cracking: searches logs of consecutive logon failures from SSH and RDP logon processes. • Port listening snapshot: takes and stores a snapshot of all listening ports at a specified time, and supports searching port listening snapshots. • Account snapshot: takes and stores a snapshot of all accounts at a specified time, and supports searching snapshots of accounts. • Process snapshots: takes and stores a snapshot of all processes that are running at a specified time, and can be used to search process snapshots.	×	Value-added

		• Process initiation: records the details of process initiation, and supports searching process initiation logs. • Network connection logs: searches records of network connections that have been initiated by an instance. Network logs • Web session logs: collects 5-tuples for Web sessions between instances and networks, and supports searching Web session content. • Web access logs: captures HTTP access logs of a website, and supports searching web access logs. This feature currently does not support HTTPS access logs. • DNS logs: searches outbound Domain Name System (DNS) request logs. This feature currently does not support private DNS servers.		

3 Scenarios

Threat Detection Service (TDS) can be used in the following scenarios:

- Real-time monitoring of business security in the cloud. TDS can generate alarms for security events such as unusual logons, webshell injections, and malware.
- Periodic vulnerability detection and baseline check for cloud services. TDS can provide vulnerability and insecure configuration detection and fixing services.
- Query, statistics, and analysis of network logs, server logs, and user visits.
- Real-time monitoring of open ports on ECS instances and security issues, including AccessKey leaks, network intrusions, DDoS attacks, and bots.
- Tracking of intrusions, such as webshell injections, malware, and ransomware in ECS, to analyze the patterns of intrusions and locate the causes.