TR-4645：安全功能

StorageGRID solutions and resources

NetApp
December 12, 2025

目录

TR-4645：安全功能

保护对象存储中的StorageGRID数据和元数据的安全

了解StorageGRID对象存储解决方案不可或缺的安全功能。

这是NetApp® StorageGRID® 中众多安全功能的概述，涵盖数据访问、对象和元数据、管理访问和平台安全。它已更新，包含StorageGRID 12.0 发布的最新功能。

安全性是NetApp StorageGRID对象存储解决方案不可或缺的一部分。安全性尤为重要、因为非常适合对象存储的许多类型的富内容数据在本质上也是敏感的、并受法规和合规性的约束。随着StorageGRID功能的不断发展、该软件提供了许多安全功能、这些功能对于保护组织的安全防护以及帮助组织遵守行业最佳实践至关重要。

本文概述了StorageGRID 12.0 中的众多安全功能，分为五类：

- 数据访问安全功能
- 对象和元数据安全功能
- 管理安全性功能
- 平台安全功能
- 云集成

本文旨在成为一份安全数据表——它没有详细说明如何配置系统以支持其中列举的默认未配置的安全功能。这"《StorageGRID加强指南》"可在官方 "StorageGRID 文档"页。

除了本报告中介绍的功能之外，StorageGRID还遵循 "NetApp产品安全漏洞响应和通知策略"。根据产品安全事件响应流程、对报告的漏洞进行验证和响应。

NetApp StorageGRID可为要求苛刻的企业对象存储用例提供高级安全功能。

从何处查找追加信息

要了解有关本文档中所述信息的更多信息，请查看以下文档和 / 或网站：

- NetApp StorageGRID：SEC 17a-4 (f)、FIRA 4511 (c)和CFTC 1.31 (c)-(d)合规性评估 https://www.netapp.com/media/9041-ar-cohasset-netapp-storagegrid-sec-assessment.pdf
- NetApp StorageGRID NIST FIPS 140-3 内核加密认证 https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/5097
- NetApp StorageGRID NIST SP 800-90B 熵认证 https://csrc.nist.gov/projects/cryptographic-module-validation-program/entropy-validations/certificate/223
- NetApp StorageGRID加拿大网络安全中心通用准则认证 https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/565-LSS%20CT%20v1.0.pdf
- StorageGRID文档页面https://docs.netapp.com/us-en/storagegrid/[]
- NetApp产品文档 https://www.netapp.com/support-and-training/documentation/

术语和首字母缩略语

本节提供了文档中所用术语的定义。

术语或首字母缩略语	定义
S3	Simple Storage Service。
客户端	一种可以通过S3协议(用于数据访问)或HTTP协议(用于管理)与StorageGRID连接的应用程序。
租户管理员	StorageGRID租户帐户的管理员
租户用户	StorageGRID租户帐户中的用户
TLS	传输层安全性
ILM	信息生命周期管理
LAN	局域网
网格管理员	StorageGRID系统的管理员
网格	StorageGRID系统
存储分段	存储在S3中的对象的容器
LDAP	轻型目录访问协议
秒	证券和交易委员会；管理交易所成员、经纪人或交易商
这是	金融行业监管机构；遵守SEC规则17a-4 (f)的格式和媒体要求
CFTC	商品期货交易委员会；管理商品期货交易
NIST	国家标准和技术研究所

数据访问安全功能

了解StorageGRID中的数据访问安全功能。

功能	功能	影响	合规性
可配置传输层安全(TLS)	TLS会为客户端与StorageGRID网关节点、存储节点或负载平衡器端点之间的通信建立握手协议。 StorageGRID支持以下TLS密码套件： • TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • TLS_AES_256_GCM_SHA384 • DHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • AES128-GCM-SHA256 • TLS_CHACHA20_POLY1305_SHA256 • ECDHE-ECDSA-CHACHA20-POLY1305 • ECDHE-RSA-CHACHA20-POLY1305 支持TLS v1.2和1.3。 不支持 SSLv3、TLS v1.1 及更早版本。	使客户端和StorageGRID能够相互识别和身份验证、并在保密和数据完整性的情况下进行通信。确保使用最新的TLS版本。现在、您可以在"配置/安全"设置下配置这些用户的用户	—

功能	功能	影响	合规性
可配置的服务器证书(负载平衡器端点)	网格管理员可以将负载平衡器端点配置为生成或使用服务器证书。	允许使用由其标准可信证书颁发机构(Certificate Authority、CA)签名的数字证书、对每个负载平衡器端点的网格和客户端之间的对象API操作进行身份验证。	—
可配置的服务器证书(API端点)	网格管理员可以集中配置所有StorageGRID API端点、以使用由其组织的受信任CA签名的服务器证书。	允许使用由其标准可信CA签名的数字证书对客户端和网格之间的对象API操作进行身份验证。	—
多租户	StorageGRID支持每个网格包含多个租户；每个租户都有自己的命名空间。租户提供S3协议；默认情况下、对分段/容器和对象的访问仅限于帐户中的用户。租户可以拥有一个用户(例如、一个企业部署、其中每个用户都有自己的帐户)或多个用户(例如、一个服务提供商部署、其中每个帐户都是服务提供商的一家公司和一个客户)。用户可以是本地用户、也可以是联合用户；联合用户由Active Directory或轻型目录访问协议(Lightweight-Directory Access Protocol、LDAP)定义。StorageGRID提供了一个按租户显示的信息板、用户可在其中使用其本地或联合帐户凭据登录。用户可以根据网格管理员分配的配额访问有关租户使用情况的可视化报告、包括分段存储的数据和对象中的使用情况信息。具有管理权限的用户可以执行租户级别的系统管理任务、例如管理用户和组以及访问密钥。	允许StorageGRID管理员托管来自多个租户的数据、同时隔离租户访问、并通过将用户与外部身份提供程序(如Active Directory或LDAP)联盟来建立用户身份。	SEC规则17a-4 (f)CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
访问凭据的不可否认性	每个S3操作都使用唯一的租户帐户、用户和访问密钥进行标识和记录。	允许网格管理员确定由哪些个人执行哪些API操作。	—
已禁用匿名访问	默认情况下、S3帐户禁用匿名访问。请求者必须拥有租户帐户中有效用户的有效访问凭据、才能访问帐户中的分段、容器或对象。可以使用显式IAM策略启用对S3存储分段或对象的匿名访问。	允许网格管理员禁用或控制对分段/容器和对象的匿名访问。	—

功能	功能	影响	合规性
合规性WORM	旨在满足SEC规则17a-4 (f)的要求、并经过Cohasset验证。客户可以在存储分段级别实现合规性。保留期限可以延长、但绝不能减少。 信息生命周期管理(ILM)规则强制实施最低数据保护级别。	允许具有法规数据保留要求的租户对存储的对象和对象元数据启用WORM保护。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
WORm	网格管理员可以通过启用禁用客户端修改选项来启用网格范围的WORM、此选项可防止客户端覆盖或删除所有租户帐户中的对象或对象元数据。 S3租户管理员还可以通过指定IAM策略按租户、存储分段或对象前缀启用WORM、此策略包括自定义的对象和元数据覆盖S3：PutOverwriteObject权限。	允许网格管理员和租户管理员控制对已存储对象和对象元数据的WORM保护。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
Kms主机服务器加密密钥管理	网格管理员可以在网格管理器中配置一个或多个外部密钥管理服务器(KMS)、以便为StorageGRID服务和存储设备提供加密密钥。每个KMS主机服务器或KMS主机服务器集群都使用密钥管理互操作性协议(Key Management互操作性协议、KMIP)为关联StorageGRID站点上的设备节点提供加密密钥。	实现空闲数据加密。对设备卷进行加密后、您将无法访问设备上的任何数据、除非节点可以与KMS主机服务器进行通信。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
自动故障转移	StorageGRID提供内置冗余和自动故障转移功能。即使从磁盘或节点到整个站点发生多个故障、也可以继续访问租户帐户、分段和对象。StorageGRID具有资源感知能力、可自动将请求重定向到可用节点和数据位置。StorageGRID站点甚至可以在隔离模式下运行；如果WAN中断使站点与系统的其余部分断开连接、则可以使用本地资源继续执行读取和写入操作、并在WAN还原后自动恢复复制。	支持网格管理员解决正常运行时间、SLA和其他合同义务问题、并实施业务连续性计划。	—

功能	功能	影响	合规性
特定于**S3**的数据访问安全功能	AWS签名版本2和版本4	对API请求签名可为S3 API操作提供身份验证。Amazon支持签名版本2和版本4的两个版本。签名过程可验证请求者的身份、保护传输中的数据并防止潜在的重放攻击。	符合AWS对签名版本4的建议、并支持与签名版本2中的旧应用程序向后兼容。
—	S3 对象锁定	StorageGRID中的S3对象锁定功能是一种对象保护解决方案、相当于Amazon S3中的S3对象锁定。	允许租户在启用S3对象锁定的情况下创建分段、以符合要求将某些对象保留固定时间或无限期的法规要求。
SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)	S3凭据的安全存储	S3访问密钥以受密码哈希功能(SHA-2)保护的格式存储。	通过组合使用密钥长度(10^{31}随机生成的数字)和密码哈希算法来安全存储访问密钥。
—	有时间限制的S3访问密钥	在为用户创建S3访问密钥时、客户可以设置访问密钥的到期日期和时间。	为网格管理员提供配置临时S3访问密钥的选项。
—	每个用户帐户具有多个访问密钥	通过StorageGRID、可以为一个用户帐户创建多个访问密钥、并使其同时处于活动状态。由于每个API操作都使用租户用户帐户和访问密钥进行记录、因此、即使多个密钥处于活动状态、也会保留不可否认性。	使客户端能够无干扰地轮换访问密钥、并允许每个客户端都有自己的密钥、从而避免在客户端之间共享密钥。
—	S3 IAM访问策略	StorageGRID支持S3 IAM策略、支持网格管理员按租户、分段或对象前缀指定精细访问控制。StorageGRID还支持IAM策略条件和变量、从而支持更动态的访问控制策略。	允许网格管理员按用户组为整个租户指定访问控制；还允许租户用户为自己的分段和对象指定访问控制。
—	S3 安全令牌服务 API AssumeRole	StorageGRID支持 S3 STS API AssumeRole 提供具有缩小范围的权限和有限持续时间的临时安全凭证（访问密钥 ID、秘密访问密钥、会话令牌）。作为 AssumeRole API 的一部分，支持内联会话策略来进一步限制会话期间的权限。	允许租户管理员提供对对象数据的安全临时访问。

功能	功能	影响	合规性
—	简单通知服务	StorageGRID支持在对象访问时发送通知。支持以下事件类型： • s3：对象创建： • s3：对象创建：放置 • s3：对象创建：发布 • s3：对象创建：复制 • s3：对象创建：完成分段上传 • s3：对象已移除： • s3：对象已移除：删除 • s3：对象已移除：删除标记已创建 • s3：对象恢复：发布	允许租户管理员监控对象的访问
—	使用StorageGRID托管密钥(SSE)进行服务器端加密	StorageGRID支持SSE、可使用StorageGRID管理的加密密钥对空闲数据进行多租户保护。	允许租户对对象进行加密。要写入和检索这些对象、需要使用加密密钥。
SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)	使用客户提供的加密密钥(SSE-C)进行服务器端加密	StorageGRID支持SSE-C、可使用客户端管理的加密密钥对空闲数据进行多租户保护。 虽然StorageGRID负责管理所有对象加密和解密操作、但使用SSE-C时、客户端必须自行管理加密密钥。	使客户端能够使用其控制的密钥对对象进行加密。要写入和检索这些对象、需要使用加密密钥。

对象和元数据安全性

了解StorageGRID中的对象和元数据安全功能。

功能	功能	影响	合规性
高级加密标准(Advanced Encryption Standard、AES)服务器端对象加密	StorageGRID可为对象提供基于AES 128和AES 256的服务器端加密。网格管理员可以启用加密作为全局默认设置。StorageGRID还支持S3 x-AMZ-server-side加密标头、以允许按对象启用或禁用加密。启用后、对象在存储时或在网格节点之间传输时会进行加密。	有助于保护对象的存储和传输、不受底层存储硬件的限制。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)

功能	功能	影响	合规性
内置密钥管理	启用加密后、每个对象都会使用随机生成的唯一对称密钥进行加密、该密钥存储在StorageGRID中、无需外部访问。	无需外部密钥管理即可启用对象加密。	
符合联邦信息处理标准(Federal Information Processing Standard、FIPS) 140-2的加密磁盘	SG5812、SG5860、SG6160和SGF6024 StorageGRID设备可提供符合FIPS 140-2的加密磁盘选项。磁盘的加密密钥可以选择由外部KMIP服务器管理。	支持安全存储系统数据、元数据和对象。此外、还提供基于StorageGRID软件的对象加密功能、可保护对象的存储和传输安全。	SEC规则17a-4 (f)CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
符合联邦信息处理标准 (FIPS) 140-3 的节点加密	SG5812、SG5860、SG6160、SGF6112、SG1100 和 SG110 StorageGRID设备提供符合 FIPS 140-3 的节点加密选项。节点的加密密钥由外部 KMIP 服务器管理。	支持安全存储系统数据、元数据和对象。此外、还提供基于StorageGRID软件的对象加密功能、可保护对象的存储和传输安全。	SEC规则17a-4 (f)CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
后台完整性扫描和自我修复	StorageGRID在对象和子对象级别使用哈希、校验和和和循环冗余校验(CrC)的互斥机制、以防止在对象存储和传输过程中出现数据不一致、篡改或修改。StorageGRID会自动检测损坏和被篡改的对象并进行替换、同时隔离更改后的数据并向管理员发出警报。	支持网格管理员满足SLA、法规和其他有关数据持久性的义务。帮助客户检测尝试加密、篡改或修改数据的勒索软件或病毒。	SEC规则17a-4 (f)CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
基于策略的对象放置和保留	StorageGRID支持网格管理员配置ILM规则、用于指定对象保留、放置、保护、过渡和到期时间。网格管理员可以将StorageGRID配置为按对象的元数据筛选对象、并在各种粒度级别应用规则、包括网格范围、租户、存储分段、密钥前缀、和用户定义的元数据键值对。StorageGRID有助于确保在对象的整个生命周期内根据ILM规则存储对象、除非客户端明确删除这些对象。	有助于强制实施数据放置、保护和保留。帮助客户在持久性、可用性和性能方面实现SLA。	SEC规则17a-4 (f)CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
后台元数据扫描	StorageGRID会定期扫描后台的对象元数据、以应用ILM指定的对象数据放置或保护更改。	帮助发现损坏的对象。	

功能	功能	影响	合规性
可调一致性	租户可以在存储分段级别选择一致性级别、以确保多站点连接等资源可用。	仅当提供所需数量的可用站点或资源时、才可选择向网格提交写入。	

管理安全性功能

了解StorageGRID中的管理安全功能。

功能	功能	影响	合规性
服务器证书(网格管理接口)	网格管理员可以将网格管理界面配置为使用由其组织的受信任CA签名的服务器证书。	允许使用由其标准可信CA签名的数字证书对管理客户端和网格之间的管理UI和API访问进行身份验证。	—
管理用户身份验证	管理用户使用用户名和密码进行身份验证。管理用户和组可以是本地用户或联合用户、也可以是从客户的Active Directory或LDAP导入的用户和组。本地帐户密码以bcrypt保护的格式存储；命令行密码以SHA-2保护的格式存储。	对管理UI和API的管理访问进行身份验证。	—
SAML支持	StorageGRID支持使用安全断言标记语言2.0 (SAML 2.0)标准的单点登录(SSO)。启用 SSO 后，所有用户都必须经过外部身份提供程序的身份验证，然后才能访问网格管理器，租户管理器，网格管理 API 或租户管理 API 。本地用户无法登录到 StorageGRID 。	为网格和租户管理员提供更高级别的安全性、例如SSO和多因素身份验证(MFA)。	NIST SP800-63
精细的权限控制	网格管理员可以为角色分配权限、并为管理用户组分配角色、这样可以使用管理UI和API强制执行允许管理客户端执行的任务。	允许网格管理员管理管理员用户和组的访问控制。	—

功能	功能	影响	合规性
分布式审核日志记录	StorageGRID提供内置的分布式审核日志记录基础架构、可扩展到多达16个站点上的数百个节点。StorageGRID软件节点会生成审核消息、这些消息通过冗余审核中继系统传输、并最终捕获到一个或多个审核日志存储库中。审核消息可捕获对象级别粒度的事件、例如客户端启动的S3 API操作、ILM对象生命周期事件、后台对象运行状况检查以及通过管理UI或API进行的配置更改。 审计日志可以通过 syslog 导出，从而允许 Splunk 和 ELK 等工具挖掘审计消息。审计消息有四种类型： • 系统审核消息 • 对象存储审核消息 • HTTP协议审核消息 • 管理审核消息 审计日志可以存储在 S3 存储桶中，以便长期保留和应用程序访问。	为网格管理员提供经验证的可扩展审计服务、使他们能够为各种目标挖掘审计数据。此类目标包括故障排除、审核SLA性能、客户端数据访问API操作以及管理配置更改。	—
系统审核	系统审核消息可捕获与系统相关的事件、例如网格节点状态、损坏对象检测、根据ILM规则在所有指定位置提交的对象以及系统范围维护任务(网格任务)的进度。	帮助客户解决系统问题、并提供根据其SLA存储对象的证据。SLA通过StorageGRID ILM规则实施、并受到完整性保护。	—
对象存储审核	对象存储审核消息可捕获对象API事务和生命周期相关事件。这些事件包括对象存储和检索、网格节点到网格节点的传输以及验证。	帮助客户审核系统中的数据进度以及是否正在交付SLA (指定为StorageGRID ILM)。	—
HTTP协议审核	HTTP协议审核消息可捕获与客户端应用程序和StorageGRID节点相关的HTTP协议交互。此外，客户还可以捕获特定的HTTP请求标头(例如X-Forwarded-for和用户元数据[x-AMZ-meta-*])以进行审核。	帮助客户审核客户端和StorageGRID之间的数据访问API操作、并跟踪单个用户帐户和访问密钥的操作。客户还可以将用户元数据记录到审核中、并使用日志挖掘工具(例如Splunk或ETK)搜索对象元数据。	—

功能	功能	影响	合规性
管理审计	管理审核消息会记录管理员用户对管理UI (网格管理接口)或API的请求。对于 API ，并非 GET 或 HEAD 请求的每个请求都会记录一个响应，其中包含 API 的用户名， IP 和请求类型。	帮助网格管理员建立系统配置更改记录、记录由哪个用户在哪个时间从哪个源IP进行更改、以及从哪个目标IP进行更改。	—
TLS 1.3支持管理UI和API访问	TLS会为管理客户端与StorageGRID管理节点之间的通信建立握手协议。	使管理客户端和StorageGRID能够相互识别和身份验证、并在机密性和数据完整性的情况下进行通信。	—
SNMPv3、用于StorageGRID监控	SNMPv3通过提供强身份验证和数据加密来保护隐私、从而提供安全性。对于v3、协议数据单元将使用CBC-DES作为加密协议进行加密。 发送协议数据单元的用户身份验证由HMAC-SHA或HMAC-MD5身份验证协议提供。 SNMPv2和v1仍受支持。	通过在管理节点上启用SNMP代理、帮助网格管理员监控StorageGRID系统。	—
Prometheus指标导出的客户端证书	网格管理员可以上传或生成客户端证书、这些证书可用于提供对StorageGRID Prometheus数据库的安全、经过身份验证的访问。	网格管理员可以使用客户端证书通过Grafana等应用程序在外部监控StorageGRID。	—

平台安全功能

了解StorageGRID中的平台安全功能。

功能	功能	影响	合规性
内部公共密钥基础架构(PKI)、节点证书和TLS	StorageGRID使用内部PKI和节点证书对节点间通信进行身份验证和加密。节点间通信受TLS保护。	有助于保护LAN或WAN上的系统流量、尤其是在多站点部署中。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
节点防火墙	StorageGRID会自动配置IP表和防火墙规则、以控制传入和传出网络流量、并关闭未使用的端口。	帮助保护StorageGRID系统、数据和元数据免受未经请求的网络流量的影响。	—

功能	功能	影响	合规性
OS强化	StorageGRID物理设备和虚拟节点的基本操作系统得到了强化；不相关的软件包将被删除。	有助于最大限度地减少潜在攻击面。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
定期更新平台和软件	StorageGRID提供常规软件版本、其中包括操作系统、应用程序二进制文件和软件更新。	有助于使用最新的软件和应用程序二进制文件保持StorageGRID系统最新。	—
已禁用通过安全Shell (SSH)进行root登录	已在所有StorageGRID节点上禁用通过SSH进行root登录。SSH访问使用证书身份验证。	帮助客户防止root登录的潜在远程密码破解。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
自动时间同步	StorageGRID会自动将每个节点的系统时钟与多个外部时间网络时间协议(NTP)服务器同步。至少需要四个Stratum 3或更高版本的NTP服务器。	确保所有节点的时间参考相同。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)
为客户端、管理和内部网格流量分隔网络	StorageGRID软件节点和硬件设备支持多个虚拟和物理网络接口、因此客户可以通过不同的网络隔离客户端、管理和内部网格流量。	允许网格管理员隔离内部和外部网络流量、并通过具有不同SLA的网络交付流量。	—
多个虚拟LAN (VLAN)接口	StorageGRID支持在StorageGRID客户端和网格网络上配置VLAN接口。	网格管理员可以对应用程序流量进行分区和隔离、以提高安全性、灵活性和性能。	
不可信客户端网络	不可信客户端网络接口仅接受已显式配置为负载平衡器端点的端口上的入站连接。	确保暴露给不可信网络的接口安全。	—
可配置防火墙	管理管理管理、网格和客户端网络的开放和关闭端口。	允许网格管理员控制端口访问、并管理经过批准的设备对端口的访问。	
增强的SSH行为	安装前默认禁用 SSH。在默认状态下，仅在链路本地管理端口地址上启用 SSH 访问。管理员和 root 用户密码设置为设备计算控制器序列号。仅允许在串行控制台和图形控制台（BMC KVM）上登录。任何网络端口上的 SSH 均被禁用。	增强网络访问保护。	SEC规则17a-4 (f) CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)

功能	功能	影响	合规性
节点加密	作为新的KMS主机服务器加密功能的一部分、StorageGRID设备安装程序会添加一个新的节点加密设置。	必须在设备安装的硬件配置阶段启用此设置。	SEC规则17a-4 (f)CTFC 1.31 (c)-（d)(FIRA)规则4511 (c)

云集成

了解StorageGRID如何与云服务集成。

功能	功能	影响
基于通知的病毒扫描	StorageGRID平台服务支持事件通知。事件通知可与外部云计算服务结合使用、用于对数据触发病毒扫描工作流。	允许租户管理员使用外部云计算服务触发数据病毒扫描。

版权信息

商标信息