目录

节点概要

CPU指令集支持

项目	值
CPU指令集	avx2（支持AVX2）

K8S节点信息

name	internal_ip	os_image	kernel_version	cpu_capacity	memory_capacity_GB	cpu_allocatable	memory_allocatable_GB	creation_timestamp
dmoc-fefcfe3fc68e	100.255.255.21	PlatOS 1.3 (LTS)	4.19.90-25.17.230.po1.x86_64	32	251.36	29	242.36	2025-10-16T06:40:01Z
dmoc-fefcfe633515	100.255.255.24	PlatOS 1.3 (LTS)	4.19.90-25.17.230.po1.x86_64	32	251.36	29	242.36	2025-10-16T06:40:14Z
dmoc-fefcfe77fdd9	100.255.255.22	PlatOS 1.3 (LTS)	4.19.90-25.17.230.po1.x86_64	32	251.36	29	242.36	2025-10-16T06:40:15Z
dmoc-fefcfea2f8d9	100.255.255.23	PlatOS 1.3 (LTS)	4.19.90-25.17.230.po1.x86_64	32	251.36	29	242.36	2025-10-16T06:39:42Z

存储卷容量(GB)

node_host	name	path	total_space_GB	free_space_GB	keep_free_space_GB
chi-pro-xdr-ck-0-0-0	default	/var/lib/clickhouse/	10158.18	4273.89	0.00
chi-pro-xdr-ck-1-0-0	default	/var/lib/clickhouse/	10158.18	4232.07	0.00
chi-pro-xdr-ck-2-0-0	default	/var/lib/clickhouse/	10158.18	4196.11	0.00
chi-pro-xdr-ck-3-0-0	default	/var/lib/clickhouse/	10158.18	4246.44	0.00

business表画像

业务TTL非180天

database	table	ttl_expression	ttl_value
business	acl_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	asset_infer_local	TTL toDate(maxRecordTimestamp) + toIntervalDay(90)	90
business	asset_log_local	TTL insertTime + toIntervalDay(30)	30
business	datalake_platform_log_local	TTL insertTime + toIntervalDay(21)	21
business	datalake_report_log_local	TTL insertTime + toIntervalDay(30)	30
business	db2_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	dce_rpc_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	dns_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	dynamic_graph_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	endpoint_behavior_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	endpoint_security_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	file_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	ftp_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365

database	table	ttl_expression	ttl_value
business	ftp_login_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	http_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	http_login_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	icmp_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	imap_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	imap_login_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	ioa_log_local	TTL toDate(collect_api_receive_time) + toIntervalDay(365)	365
business	ldap_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	mongo_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	mysql_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	nat_config_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	nat_session_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	network_security_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	ntlm_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	operation_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	oracle_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	pgsql_cmd_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	pgsql_login_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	pop3_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	pop3_login_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	raw_log_local	TTL toDate(recordTimestamp) + toIntervalDay(7)	7
business	rdp_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	redis_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	sas_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	smb_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	smtp_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	smtp_login_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	snmp_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	sql_server_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	ssh_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	sybase_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	tcp_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	telnet_login_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	vpn_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	weak_log_local	TTL insertTime + toIntervalDay(30)	30
business	ztna_access_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	ztna_user_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365
business	ztna_user_security_log_local	TTL toDate(recordTimestamp) + toIntervalDay(365)	365

business库数据量统计

指标	数量
数据量为0的表数量	112
数据量不为0的表数量	47

business库按未压缩大小降序Top10

database	table	engine	total_rows	compressed_size_GB	uncompressed_size_GB
business	http_log_local	MergeTree	7154939175	13988.66	45705.96
business	parse_status_log_local	ReplacingMergeTree	8896908279	790.38	10009.49
business	tcp_log_local	MergeTree	10403631207	313.43	6856.32
business	dns_log_local	MergeTree	7101429594	452.51	6467.19
business	endpoint_behavior_log_local	MergeTree	1674242156	170.95	4131.96
business	network_security_log_local	MergeTree	322393558	231.90	2887.59
business	ssl_tls_log_local	MergeTree	450151668	197.78	2693.65
business	acl_log_local	MergeTree	1509244771	117.11	1537.44
business	icmp_log_local	MergeTree	1527301404	44.71	994.62
business	ftp_log_local	MergeTree	478859072	8.91	306.93

非人工用户组查询时间范围PXX Top10

table_name	p50_days	p80_days	p90_days	p95_days	p99_days
network_security_log	1	1	1	29	29
endpoint_security_log	1	1	1	1	29
__ALL__	1	1	1	1	2
endpoint_behavior_log	2	2	2	2	2
http_log	1	1	1	1	1
ioa_log	1	1	1	1	1
dns_log	1	1	1	1	1
tcp_log	1	1	1	1	1
icmp_log	1	1	1	1	1
redis_log	1	1	1	1	1

其他表

非business库表列表

database	table
dspm	data_security_log
dspm	data_security_log_backend
dspm	data_security_log_backend_local
dspm	data_security_log_local
dspm	http_log_statistics_by_day
dspm	http_log_statistics_by_day_local
dspm	http_log_statistics_by_day_mv
dspm	label_count_by_day
dspm	label_count_by_day_local
dspm	label_count_by_day_mv
log_checker	logcheck_ability_alert
log_checker	logcheck_ability_alert_distributed
log_checker	logcheck_ability_log

database	table
log_checker	logcheck_ability_log_distributed
log_checker	logcheck_analyze_audit_log
log_checker	logcheck_analyze_audit_log_distributed
log_checker	logcheck_analyze_security_log
log_checker	logcheck_analyze_security_log_distributed
log_checker	logcheck_business_alert
log_checker	logcheck_business_alert_distributed
log_checker	logcheck_business_incident
log_checker	logcheck_business_incident_distributed
log_checker	logcheck_datalake_audit_collect
log_checker	logcheck_datalake_audit_collect_distributed
log_checker	logcheck_datalake_audit_ingest
log_checker	logcheck_datalake_audit_ingest_distributed
log_checker	logcheck_datalake_collect
log_checker	logcheck_datalake_collect_distributed
log_checker	logcheck_datalake_ingest
log_checker	logcheck_datalake_ingest_distributed
log_checker	logcheck_enaane_alert
log_checker	logcheck_enaane_alert_distributed
log_checker	logcheck_enaane_incident
log_checker	logcheck_enaane_incident_distributed
log_checker	logcheck_mss_alert
log_checker	logcheck_mss_alert_distributed
log_checker	logcheck_mss_incident
log_checker	logcheck_mss_incident_distributed
log_checker	logcheck_result_5min
log_checker	logcheck_result_5min_distributed
metric	.inner_id.f0182d02-2d07-49f3-bcd4-31e665724936
metric	dev_report_status
metric	dev_report_status_local

视图DDL

database	view	engine	create_table_query_one_line
dspm	http_log_statistics_by_day_mv	MaterializedView	CREATE MATERIALIZED VIEW dspm.http_log_statistics_by_day_mv TO dspm.http_log_statistics_by_day_local (`createDay` DateTime, `xSrcIp` LowCardinality(String), `xDstIp` LowCardinality(String), `srcIpTag` Int32, `dstPort` Int32, `apiId` String, `xAppId` String, `accountId` String, `xUserId` String, `xUserGroupId` String, `countCountState` AggregateFunction(count, UInt8)) AS SELECT toStartOfDay(toDateTime(recordTimestamp)) AS createDay, srcIp AS xSrcIp, dstIp AS xDstIp, srcIpTag, dstPort, apiId, xAppId, accountId, xUserId, xUserGroupId, countState(1) AS countCountState FROM business.dsp_http_log_local WHERE (xAppId IS NOT NULL) AND (xAppId != '') AND (apiId IS NOT NULL) AND (apiId != '') GROUP BY createDay, xAppId, apiId, srcIp, dstIp, accountId, xUserId, xUserGroupId, srcIpTag, dstPort

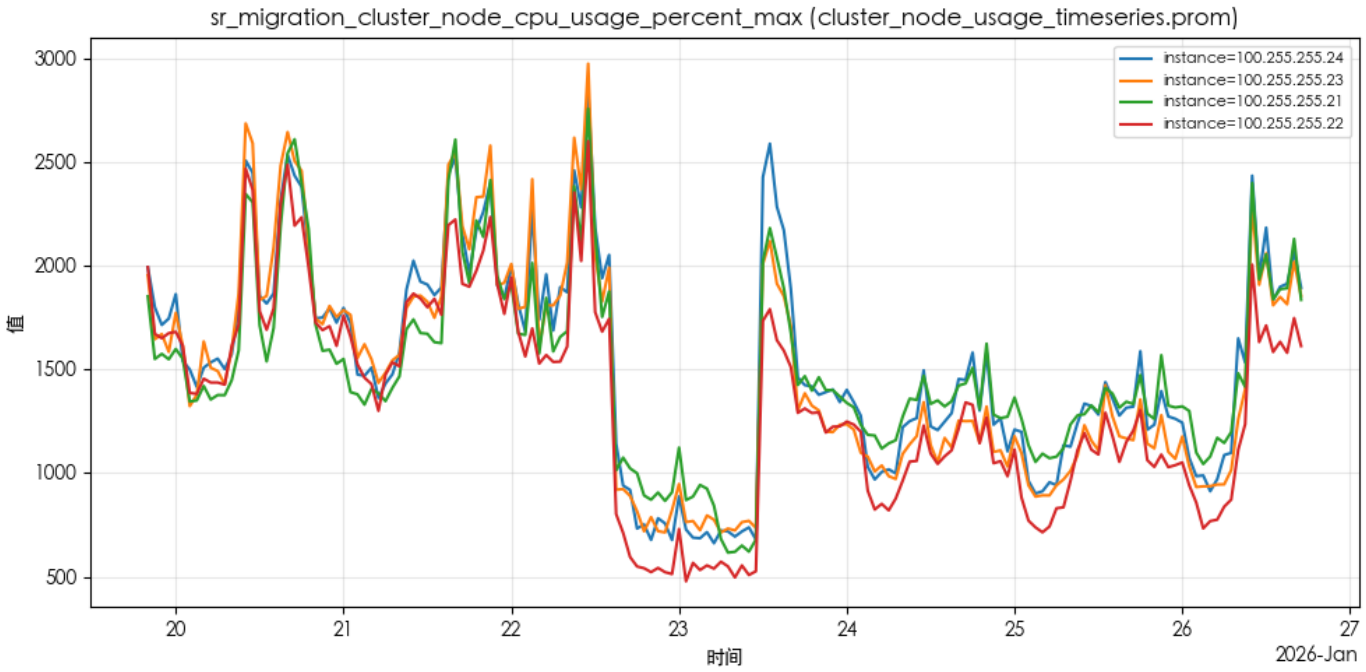
database	view	engine	create_table_query_one_line
dspm	label_count_by_day_mv	MaterializedView	CREATE MATERIALIZED VIEW dspm.label_count_by_day_mv TO dspm.label_count_by_day_local (`appId` String, `apiId` String, `accountId` String, `xForwardIp` LowCardinality(String), `srcIp` String, `dstIp` LowCardinality(String), `apiTags` Array(Int32), `srcIpTag` Int32, `userId` String, `userRole` String, `groupPath` String, `groupId` String, `createDay` DateTime, `labelId` String, `paramsType` UInt8, `labelCount` AggregateFunction(sum, Int32)) AS SELECT xAppId AS appId, apiId, accountId, business.dsp_http_log_local.srcIp AS xForwardIp, JSONExtractString(extensions, 'xSrcIp') AS srcIp, dstIp, apiTags, srcIpTag, xUserId AS userId, arrayJoin(if((length(xUserRoles) = 0) OR (xUserRoles IS NULL), [''], xUserRoles)) AS userRole, xUserGroup AS groupPath, xUserGroupId AS groupId, toDate(recordTimestamp) AS createDay, tuple.1 AS labelId, tuple.3 AS paramsType, sumState(tuple.2) AS labelCount FROM business.dsp_http_log_local ARRAY JOIN arrayConcat(arrayMap((x, y) -> (x, y, 1), respDataLabelIds, respDataCounts), arrayMap((x, y) -> (x, y, 0), reqDataLabelIds, reqDataCounts)) AS tuple WHERE (((respDataClassifications != []) AND (respDataLabelIds != [])) OR ((reqDataLabelIds != []) AND (reqDataClassifications != []))) AND (xAppId != '') AND (xAppId IS NOT NULL) AND (apiId != '') AND (apiId IS NOT NULL) AND (respDataGrade > 0) GROUP BY createDay, appId, apiId, srcIp, xForwardIp, dstIp, labelId, accountId, userId, groupId, userRole, groupPath, paramsType, apiTags, srcIpTag
metric	dev_report_status_local	MaterializedView	CREATE MATERIALIZED VIEW metric.dev_report_status_local (`tenant` LowCardinality(String), `deviceId` LowCardinality(String), `productType` LowCardinality(String), `srcIp` String, `source` LowCardinality(String), `cloudRecieveTimestamp` UInt64, `heartbeatTimestamp` UInt64) ENGINE = ReplacingMergeTree(cloudRecieveTimestamp) PARTITION BY tenant PRIMARY KEY cloudRecieveTimestamp ORDER BY (cloudRecieveTimestamp, tenant, deviceId, productType) SETTINGS allow_nullable_key = 1, index_granularity = 8192 AS SELECT tenant, deviceId, productType, srcIp, gateway AS source, max(cloudRecieveTimestamp) AS cloudRecieveTimestamp, max(heartbeatTimestamp) AS heartbeatTimestamp FROM business.report_audit_log_local GROUP BY tenant, deviceId, productType, srcIp, source

时序图

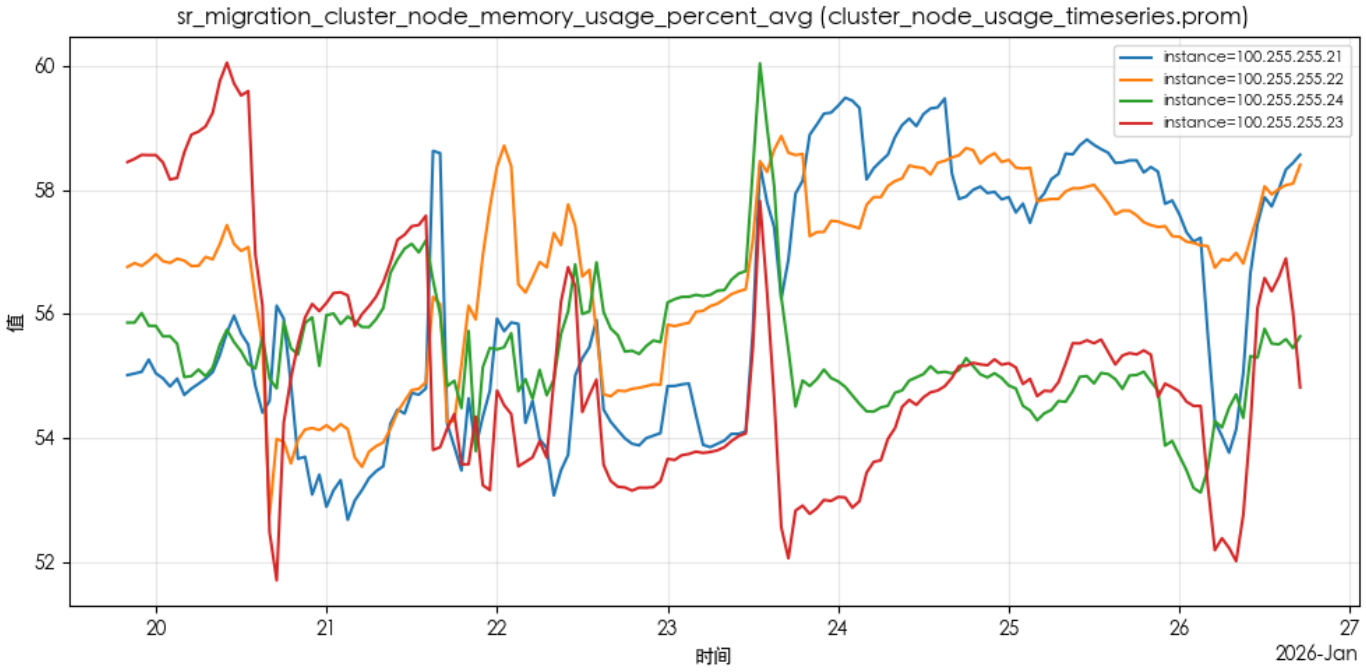
节点资源使用

说明：展示节点CPU、内存、磁盘与网络资源的平均与峰值变化趋势。

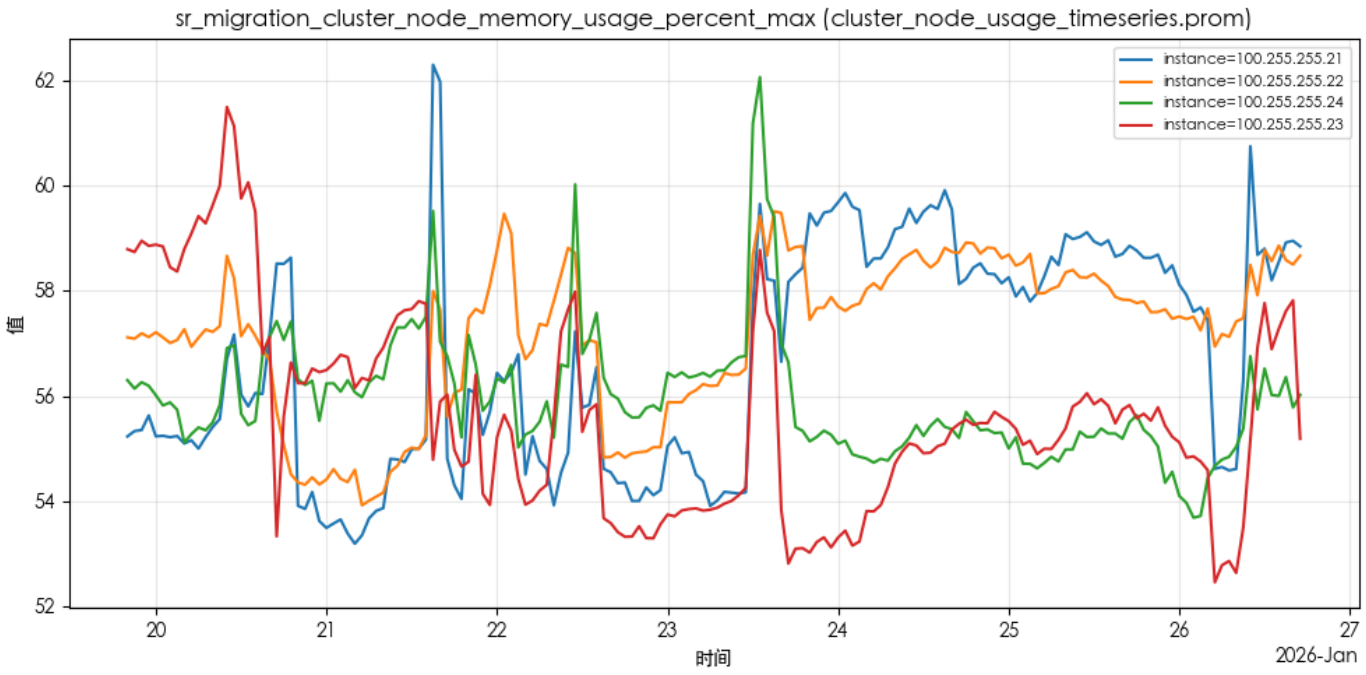
说明：节点CPU使用率平均值（非idle），用于观察CPU负载趋势。



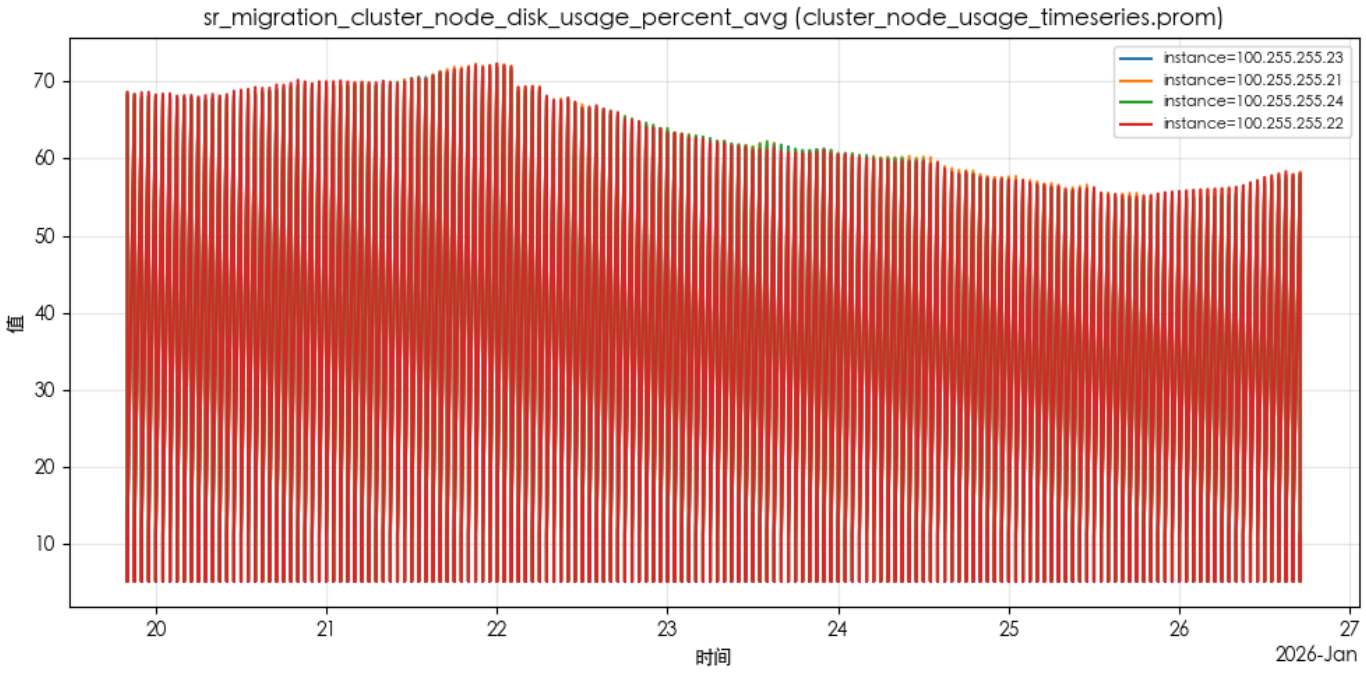
说明：节点CPU使用率峰值（非idle），用于识别CPU尖峰。



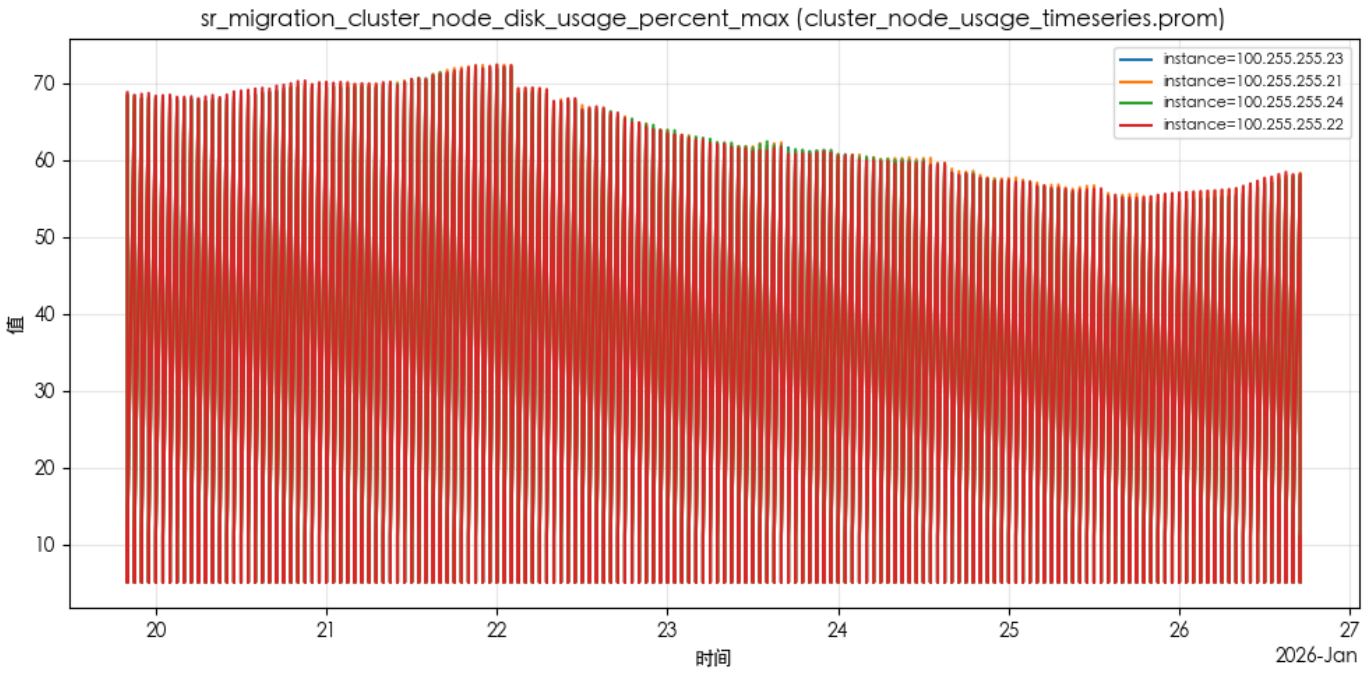
说明：节点内存使用率平均值，反映内存压力水平。



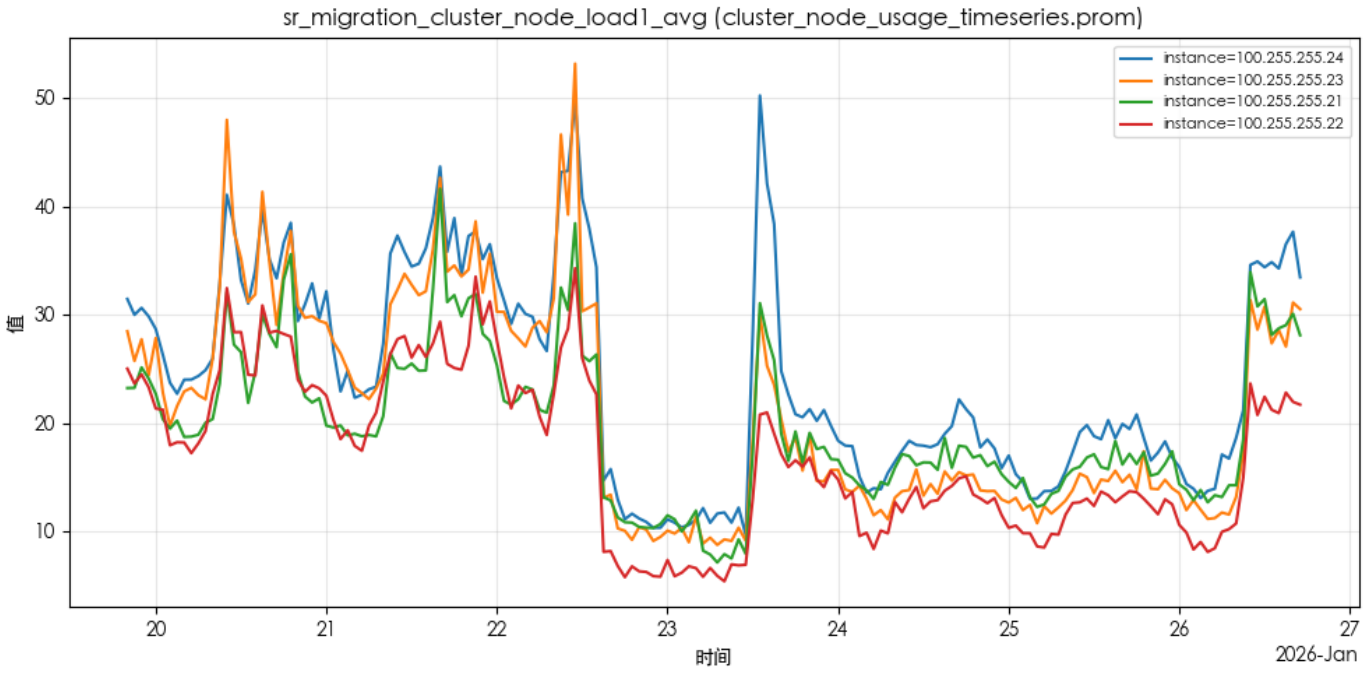
说明：节点内存使用率峰值，用于识别内存峰值。



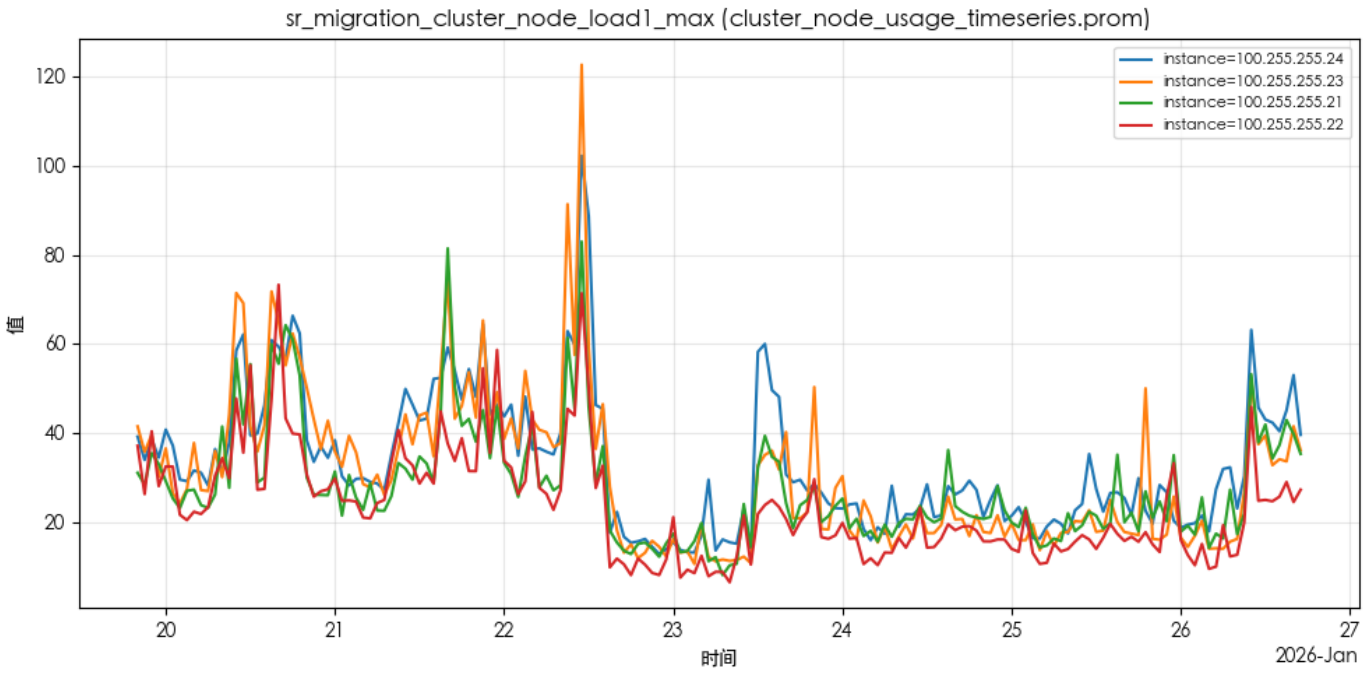
说明：节点磁盘使用率平均值，反映磁盘容量占用。



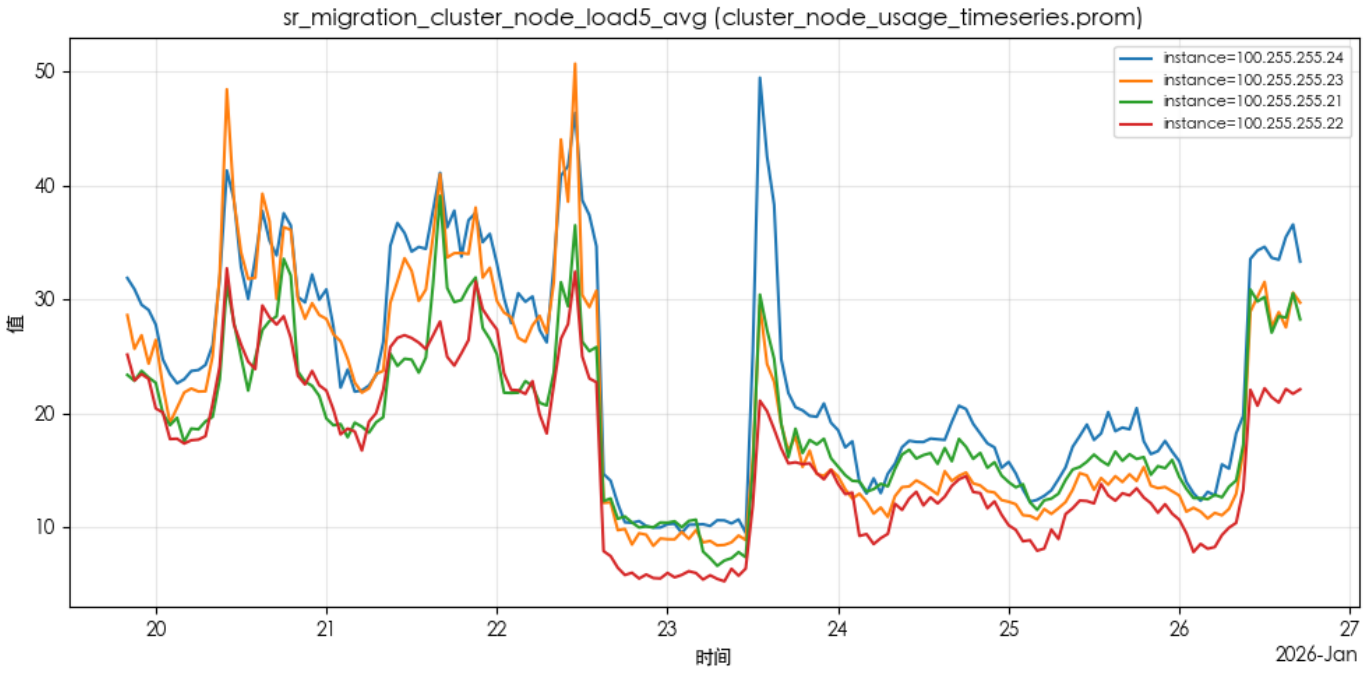
说明：节点磁盘使用率峰值，用于识别容量紧张节点。



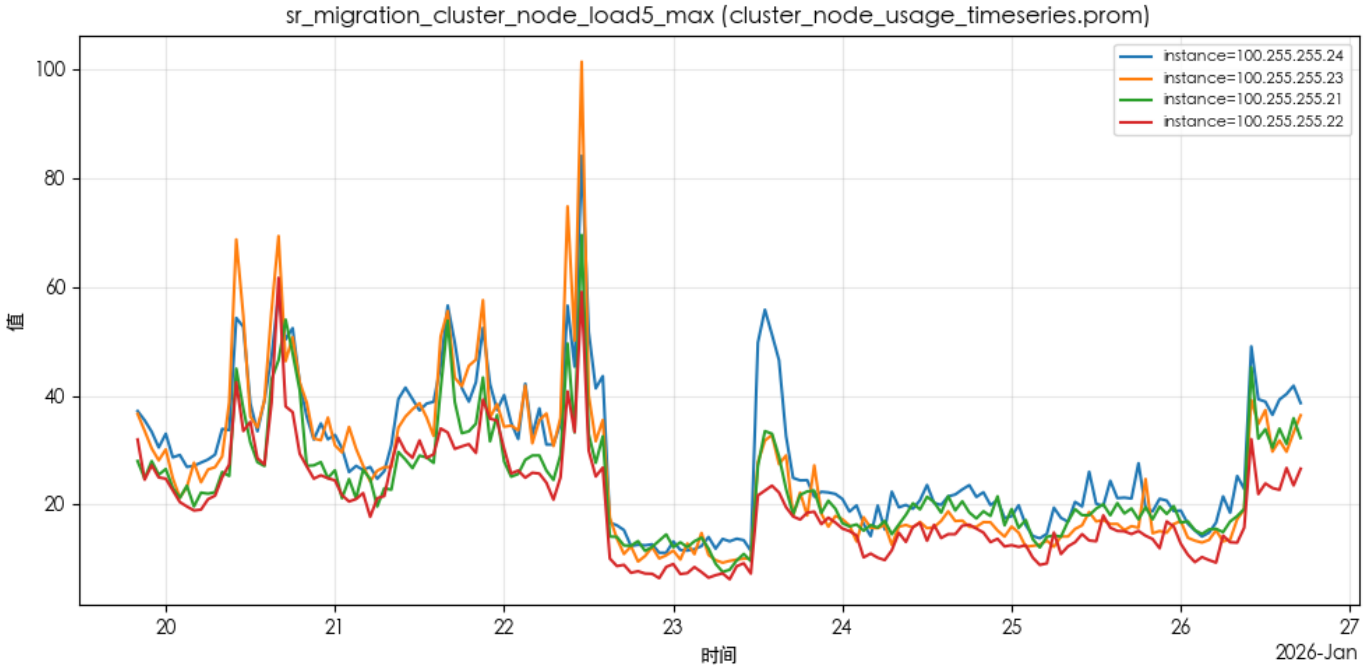
说明：节点1分钟平均负载，反映短期负载变化。



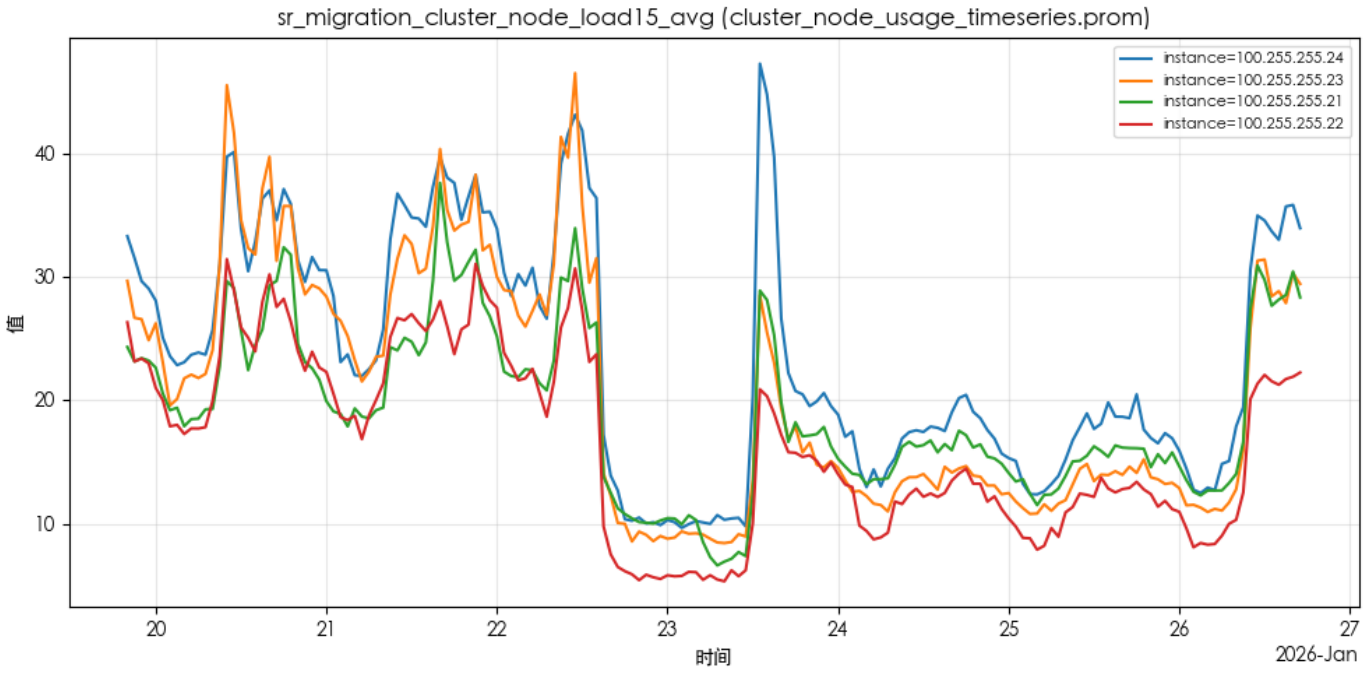
说明：节点1分钟负载峰值，用于识别短期突发负载。



说明：节点5分钟平均负载，反映中期负载水平。

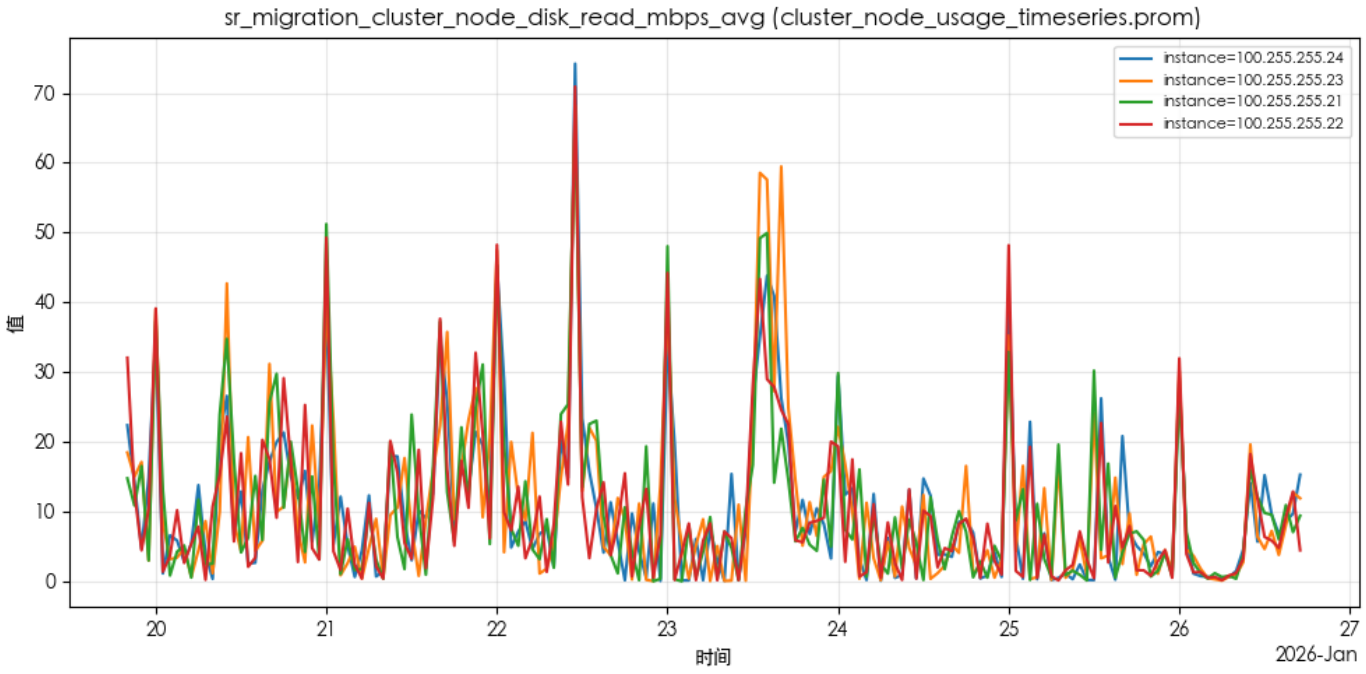


说明：节点5分钟负载峰值，用于识别持续负载高点。

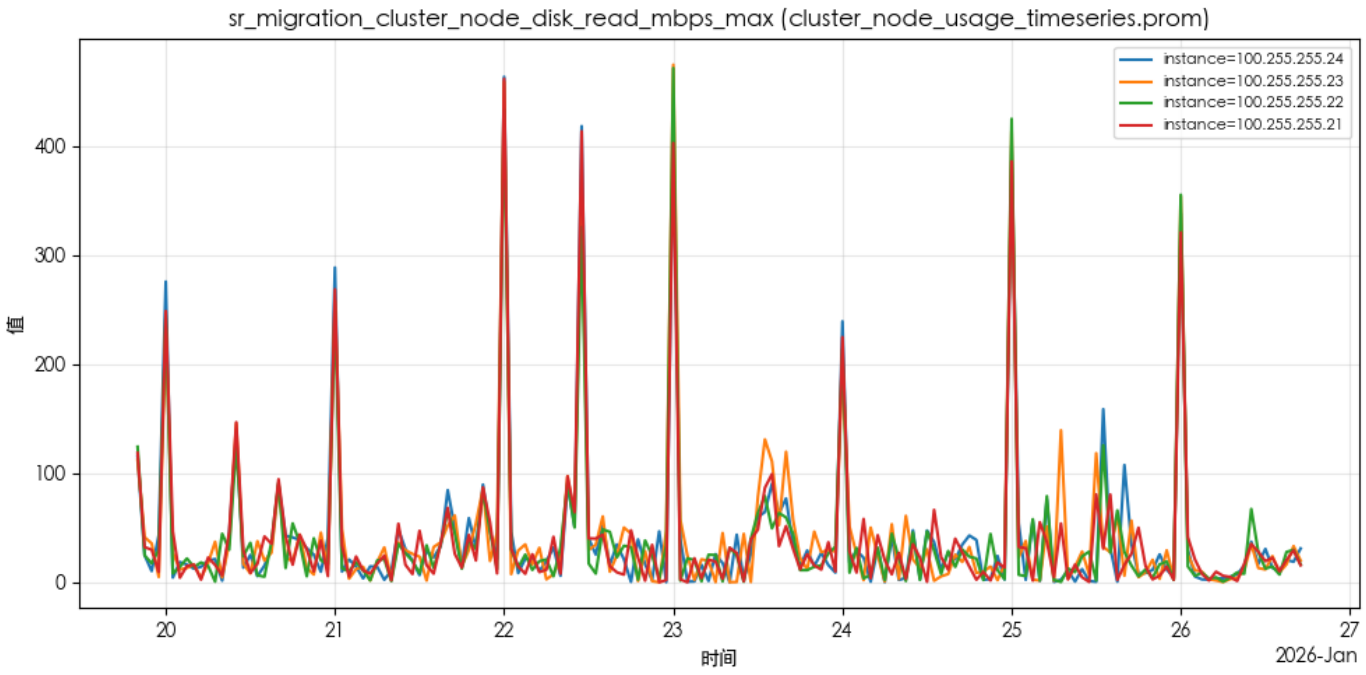


说明：节点15分钟平均负载，反映长期负载水平。

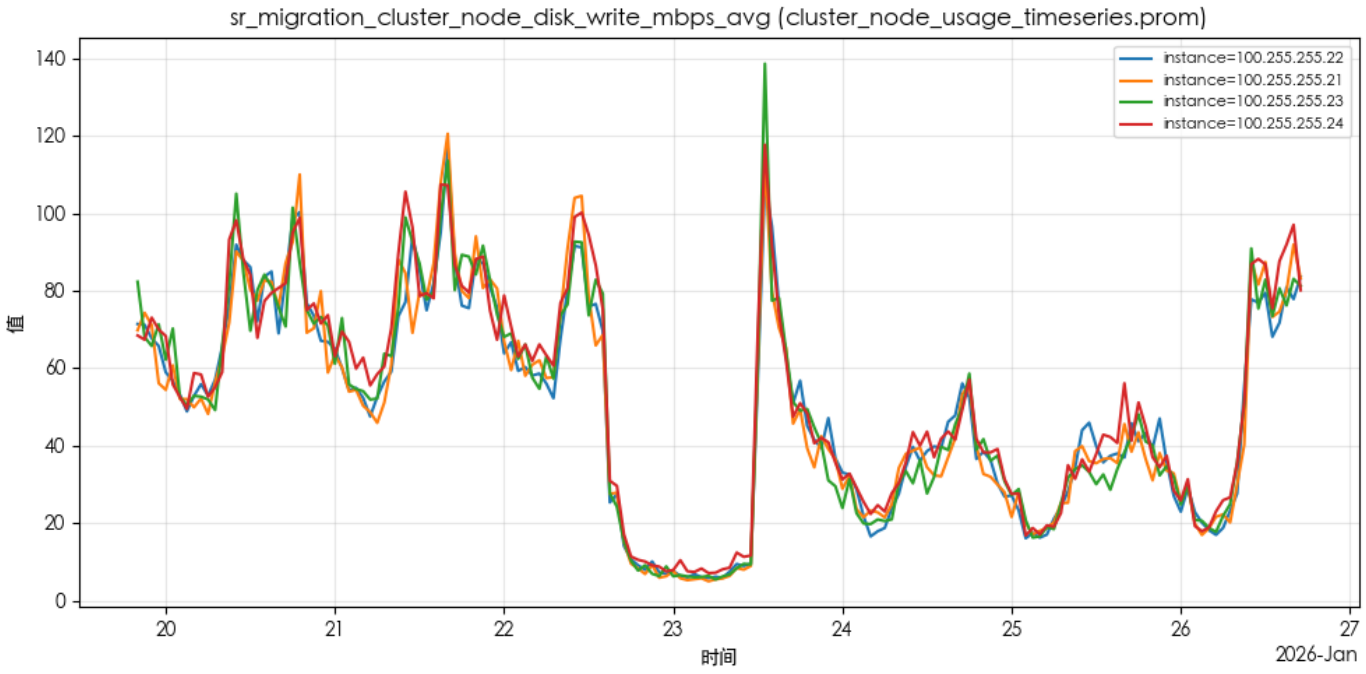
说明：节点15分钟负载峰值，用于识别长期高负载节点。



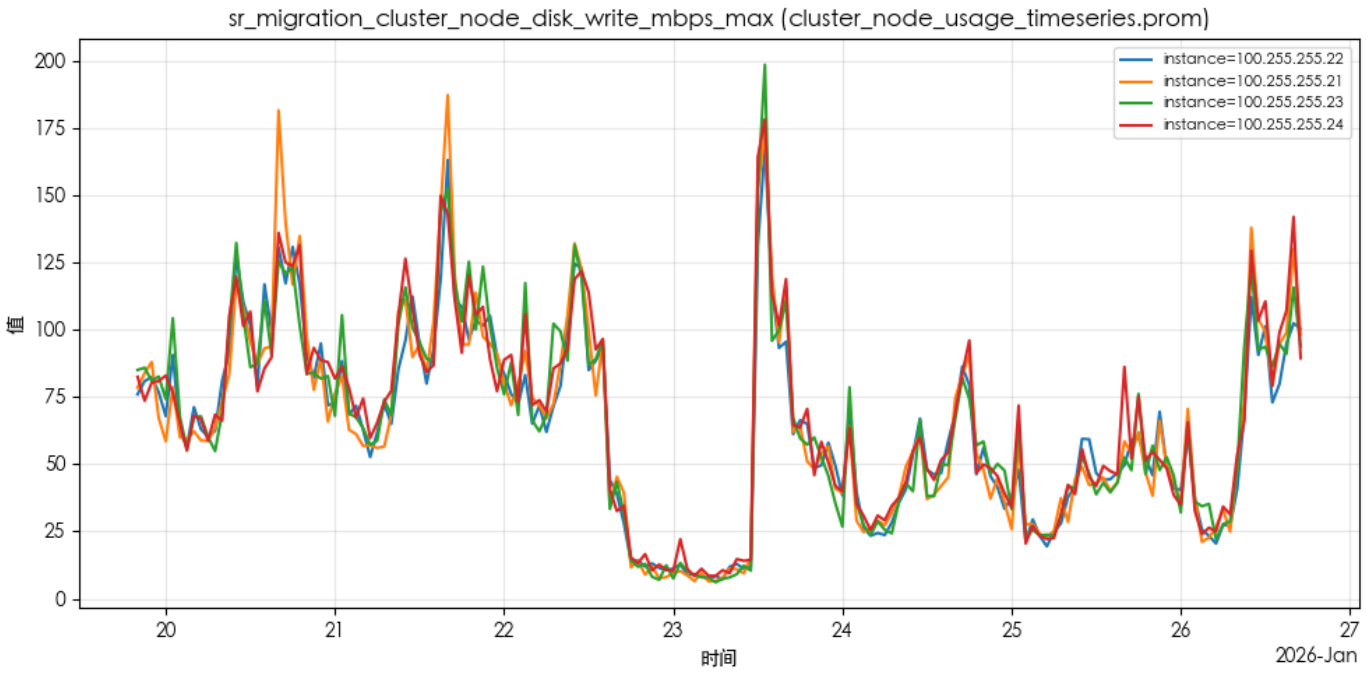
说明：节点磁盘读吞吐平均值（MB/s），反映读IO压力。



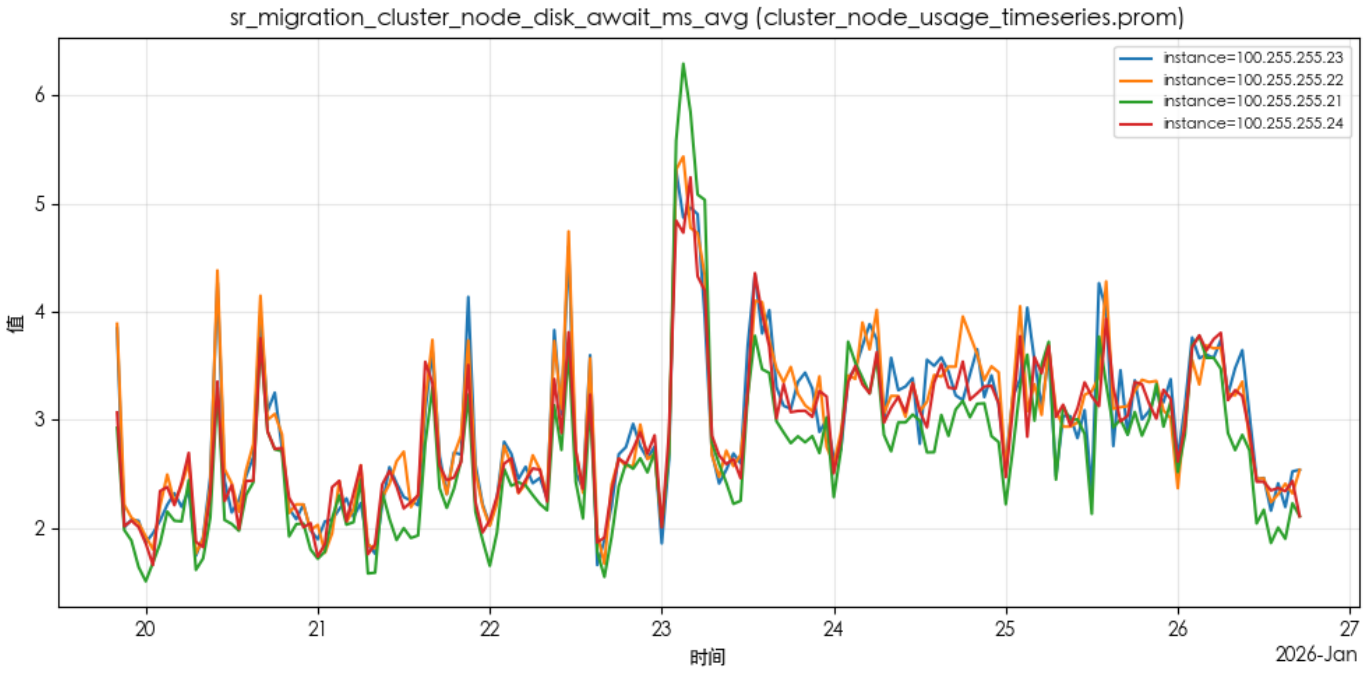
说明：节点磁盘读吞吐峰值（MB/s），用于识别读突发。



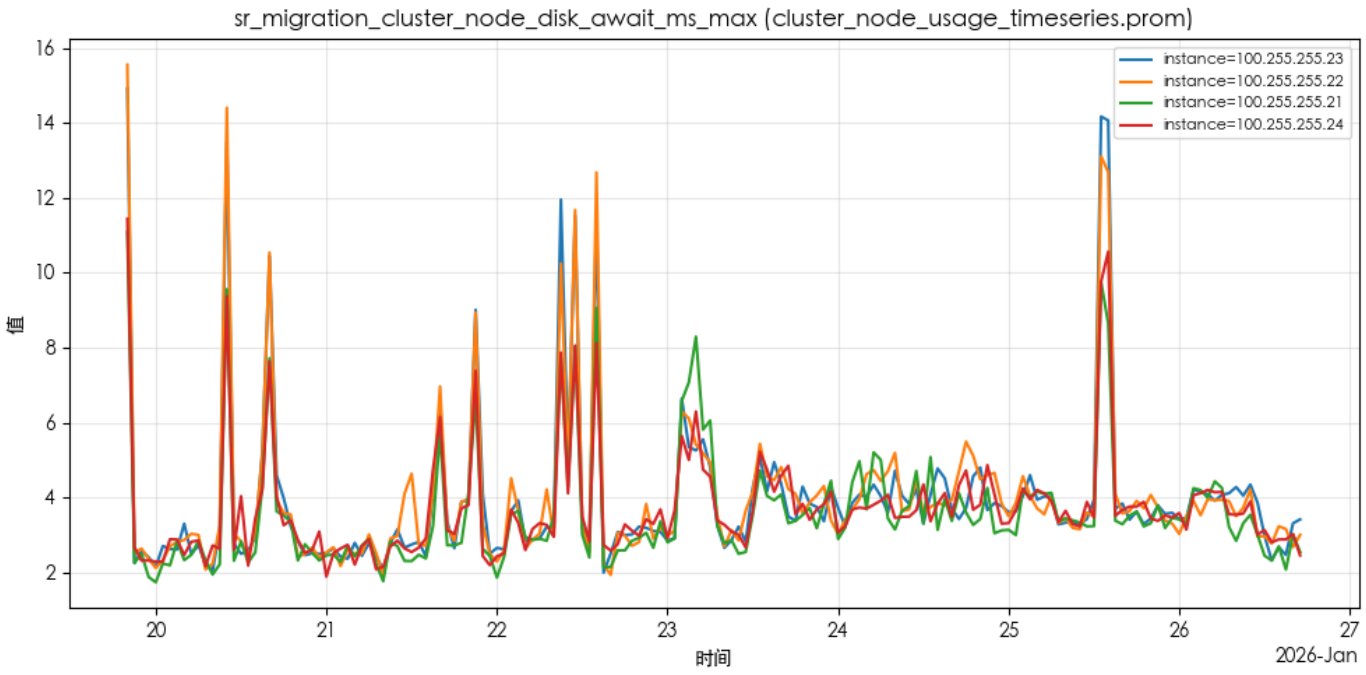
说明：节点磁盘写吞吐平均值（MB/s），反映写IO压力。



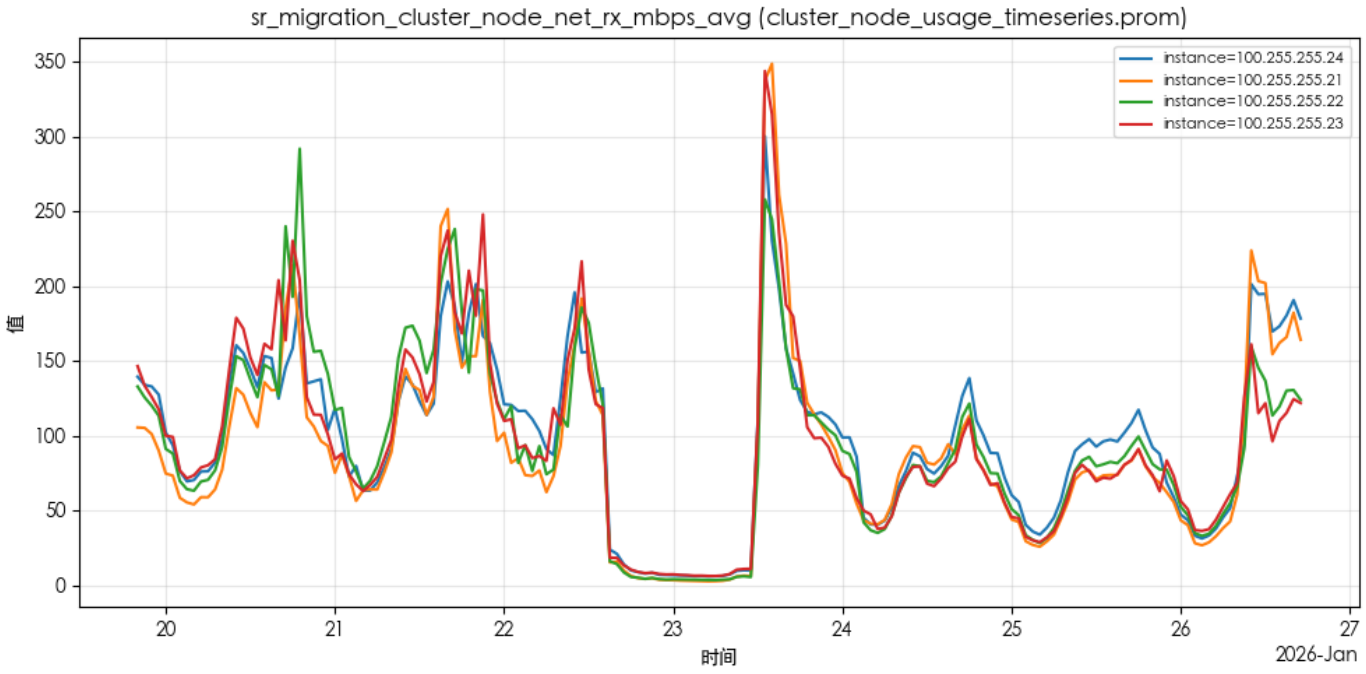
说明：节点磁盘写吞吐峰值（MB/s），用于识别写突发。



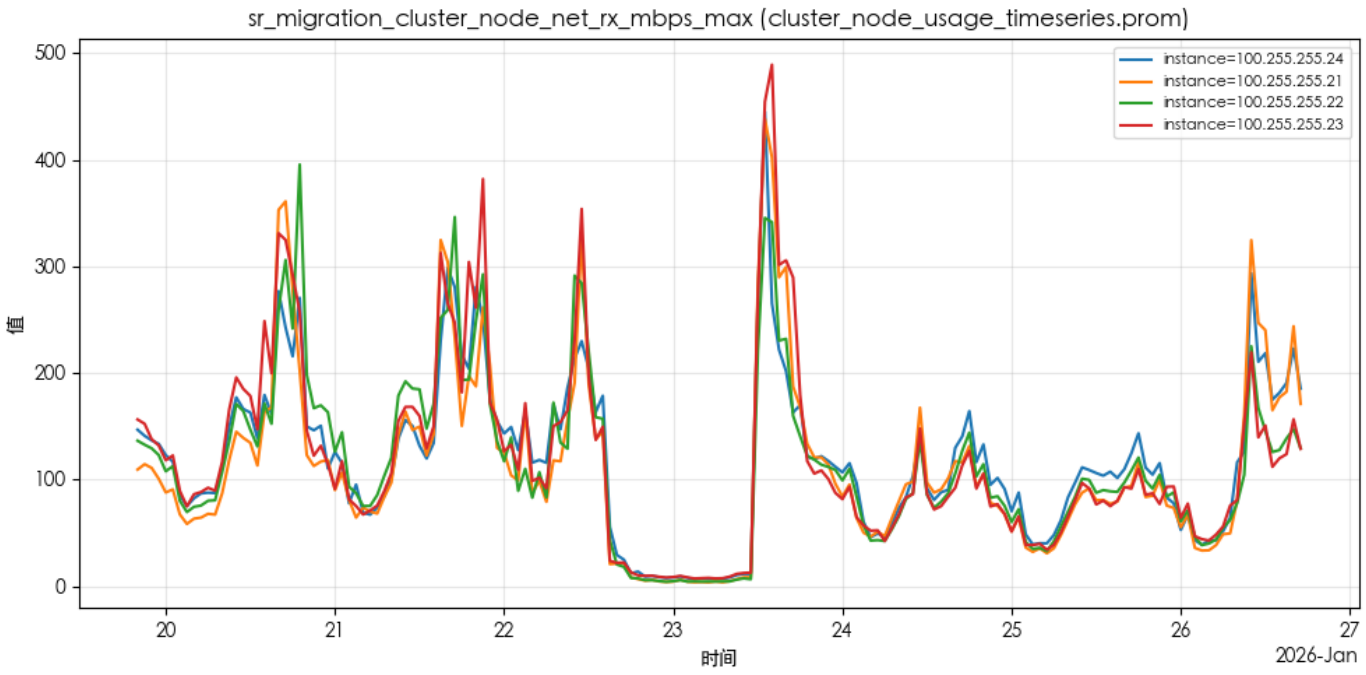
说明：节点磁盘IO等待时延平均值（ms），反映IO响应情况。



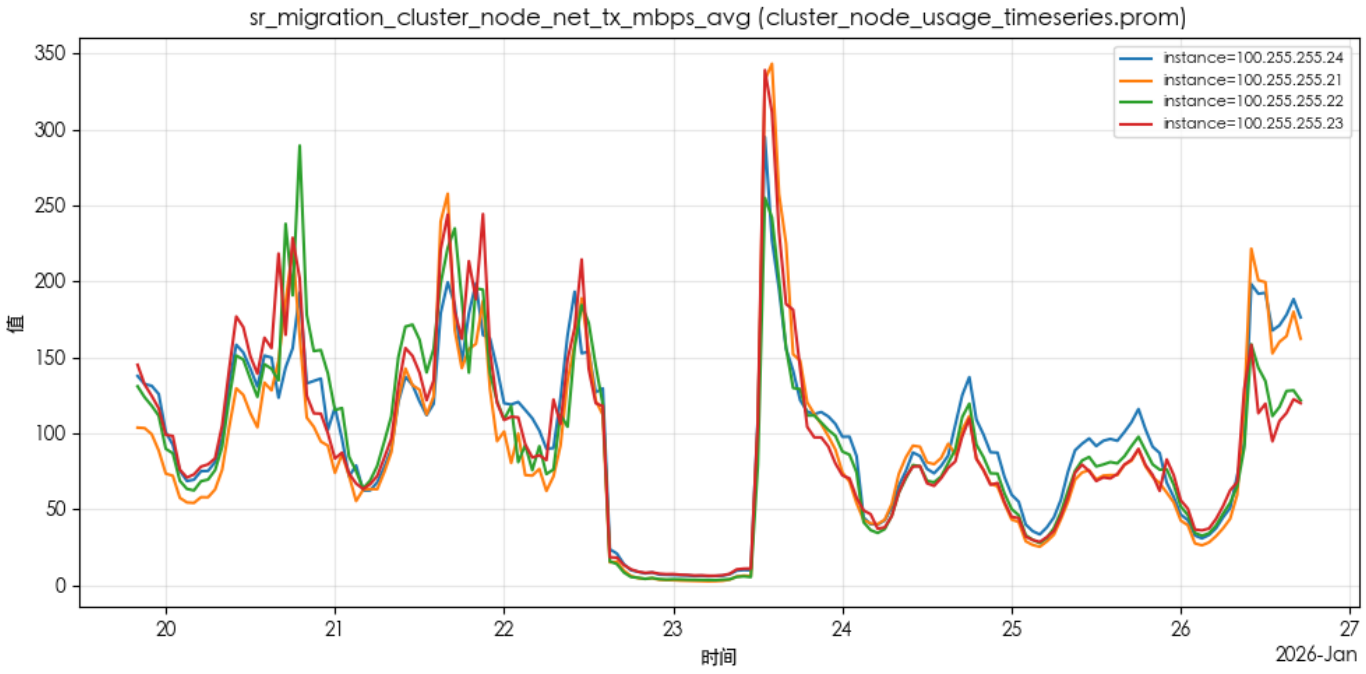
说明：节点磁盘IO等待时延峰值（ms），用于识别IO抖动。



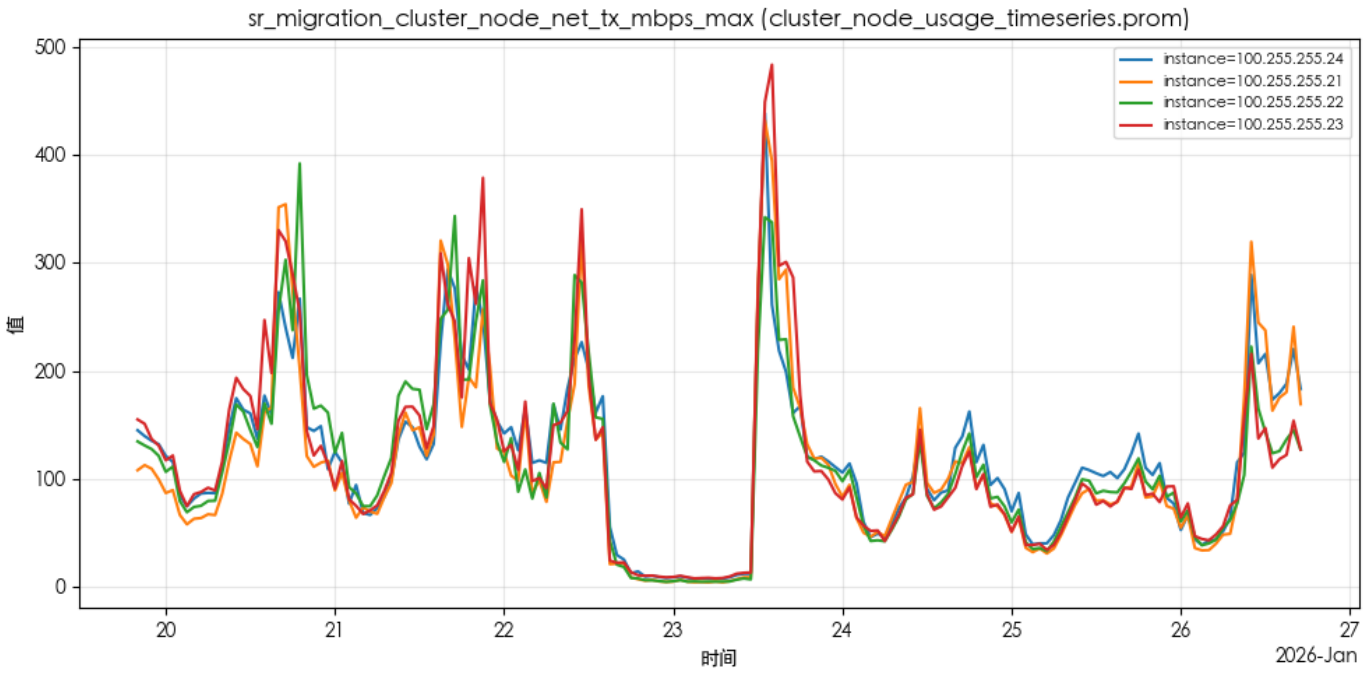
说明：节点网络接收速率平均值（MB/s），反映入站带宽使用。



说明：节点网络接收速率峰值（MB/s），用于识别入站突发流量。



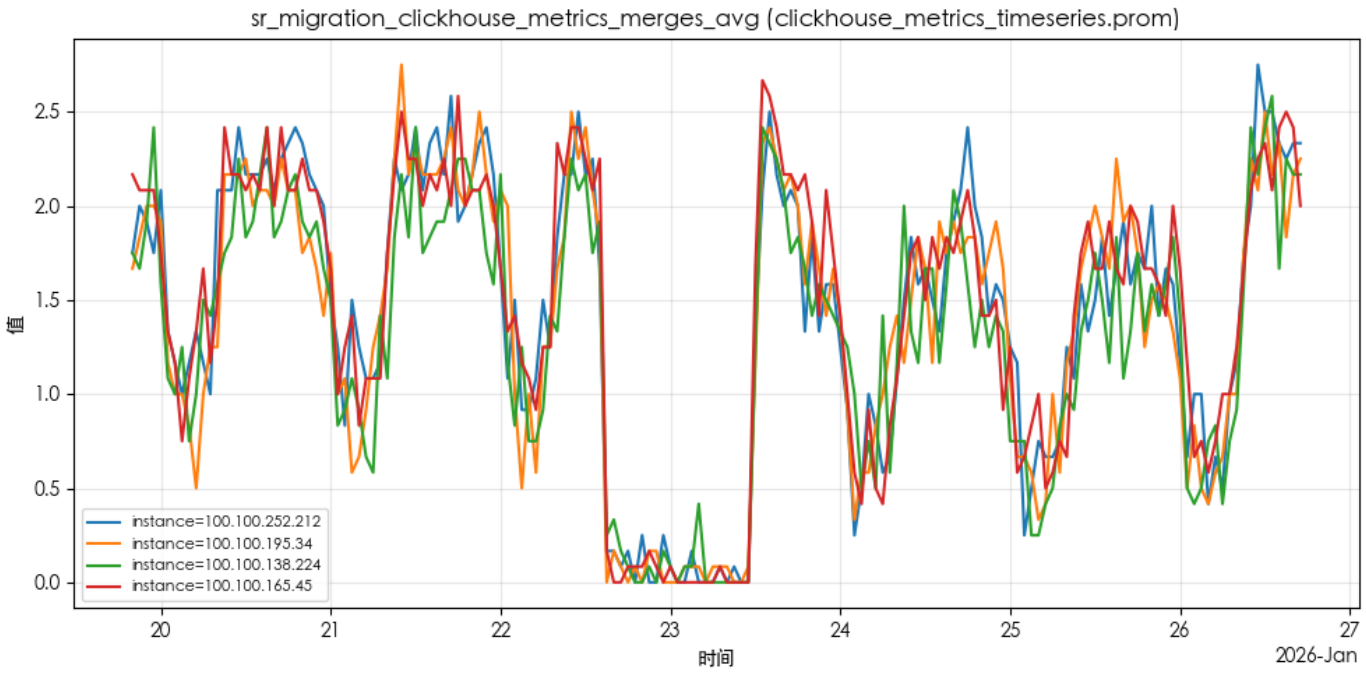
说明：节点网络发送速率平均值（MB/s），反映出站带宽使用。



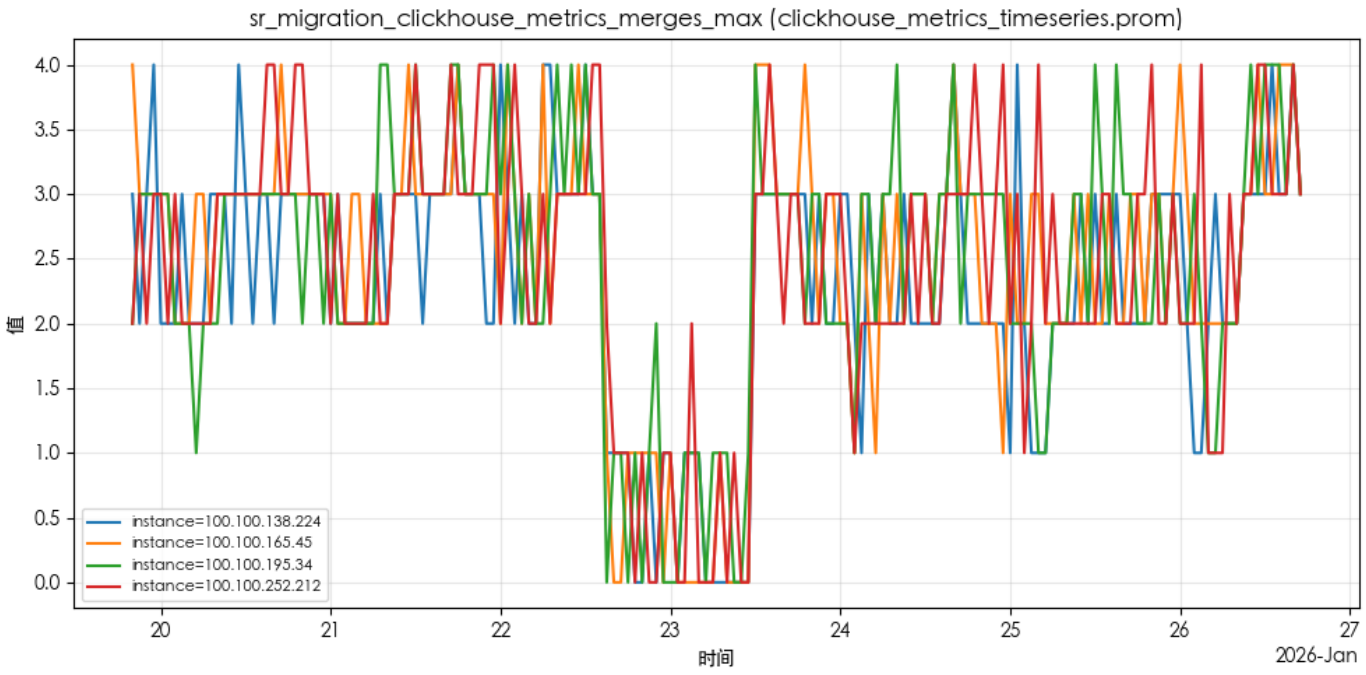
说明：节点网络发送速率峰值（MB/s），用于识别出站突发流量。

ClickHouse关键指标

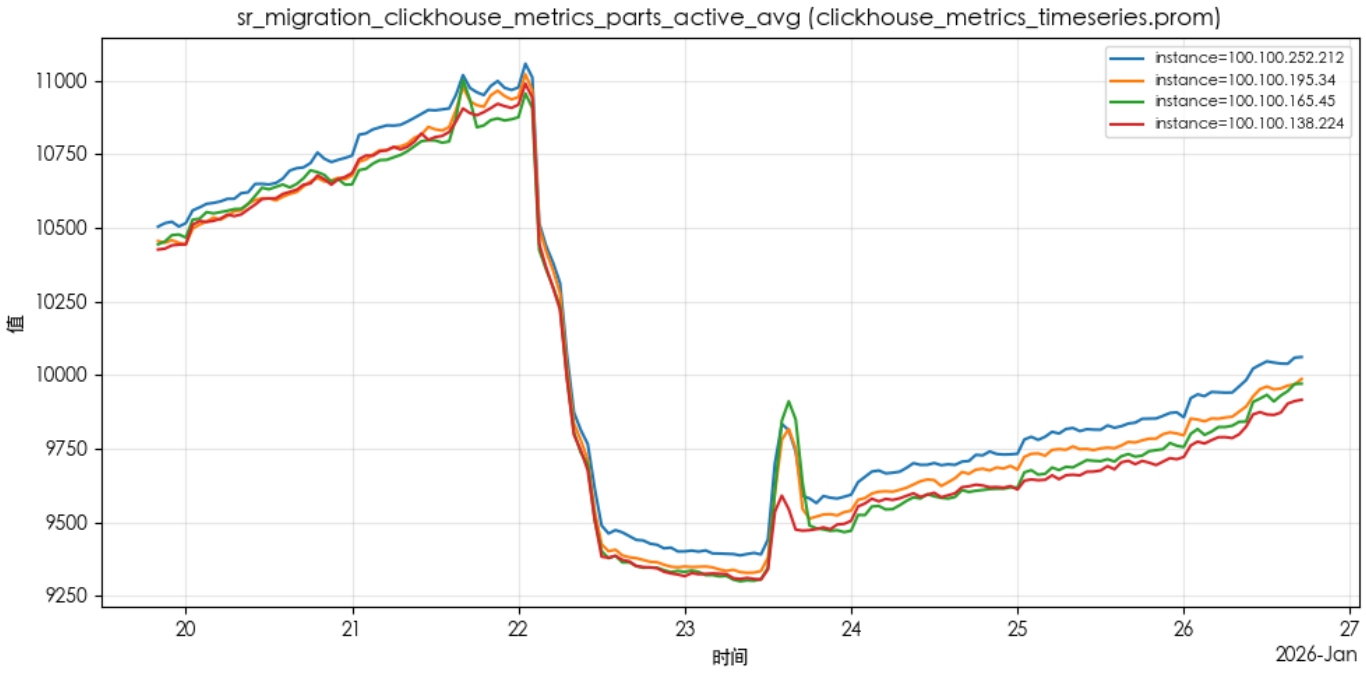
说明：展示ClickHouse核心运行指标随时间的变化，用于评估负载与稳定性。



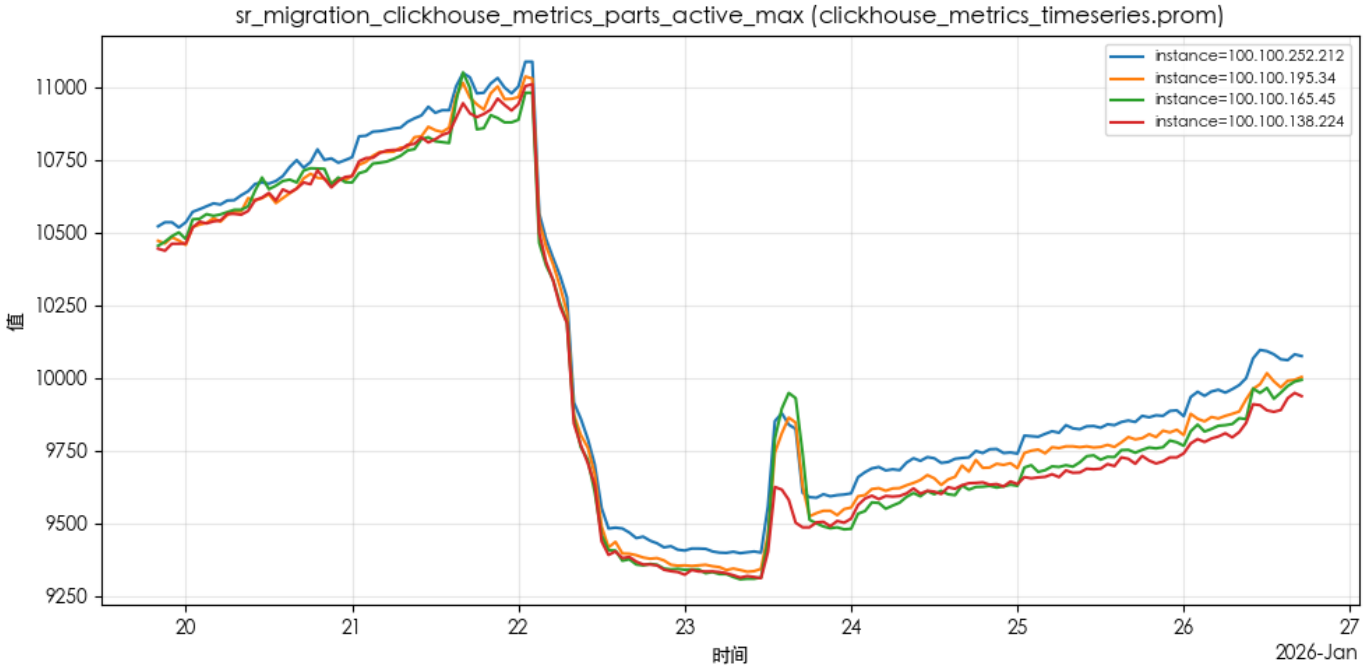
说明：ClickHouse后台合并任务数平均值，用于观察合并压力。



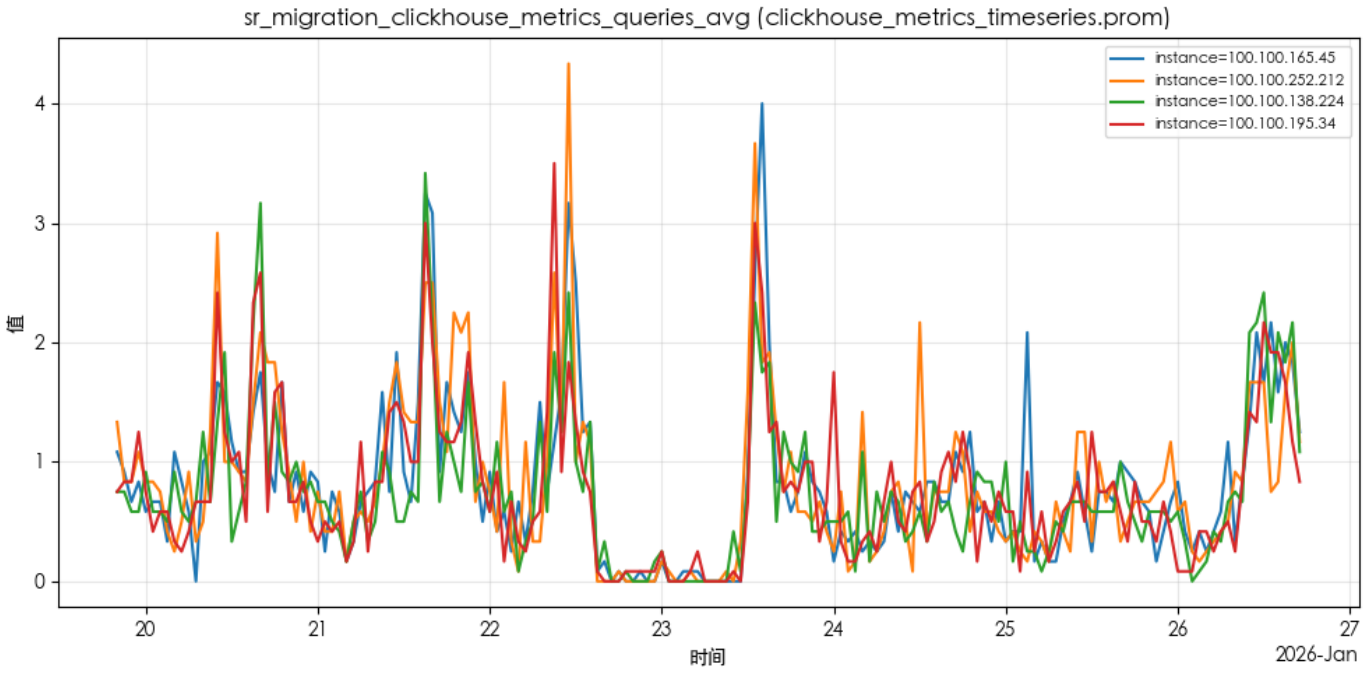
说明：ClickHouse后台合并任务数峰值，用于识别合并高峰。



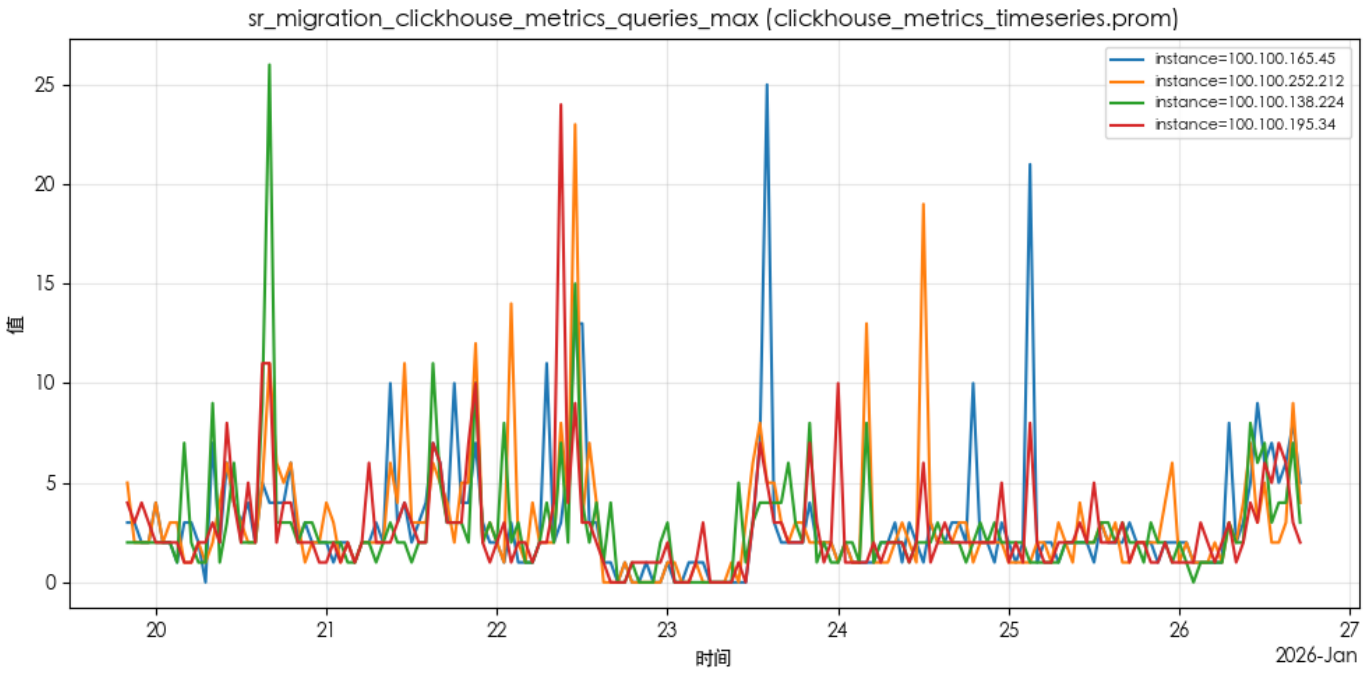
说明：活跃Part数量平均值，用于评估存储碎片情况。



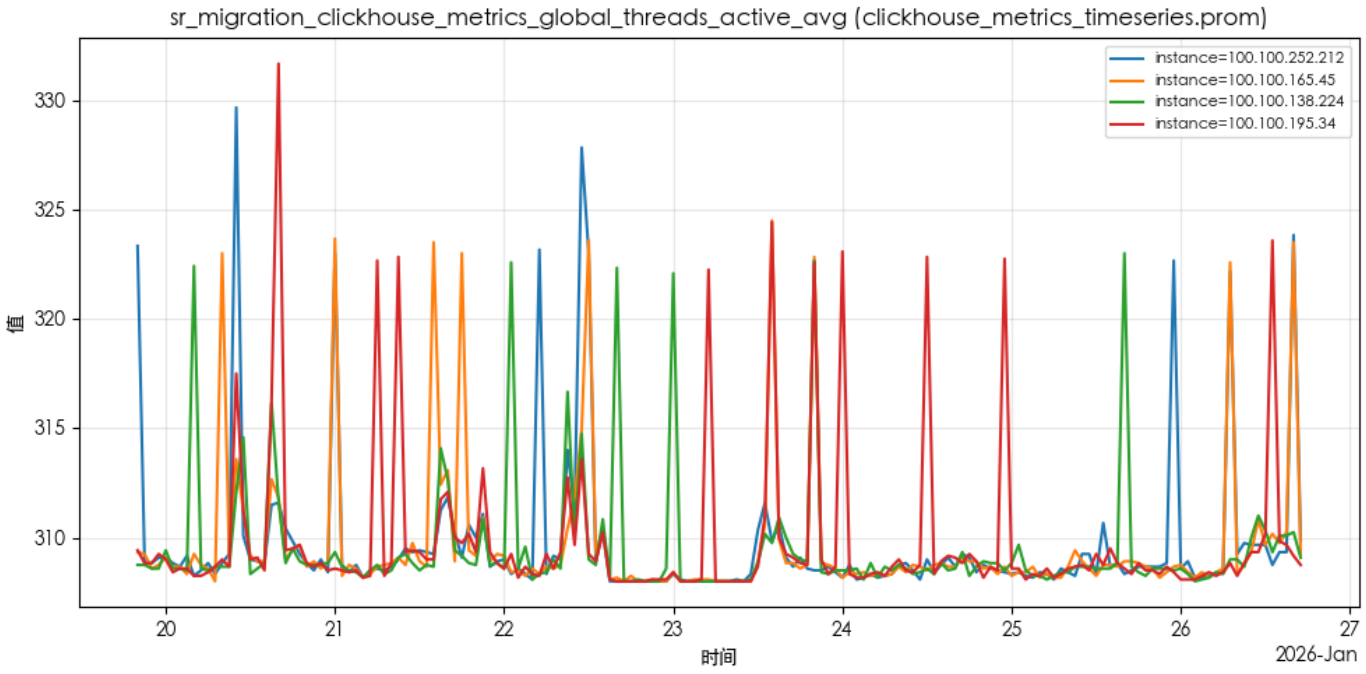
说明：活跃Part数量峰值，用于识别Part累积。



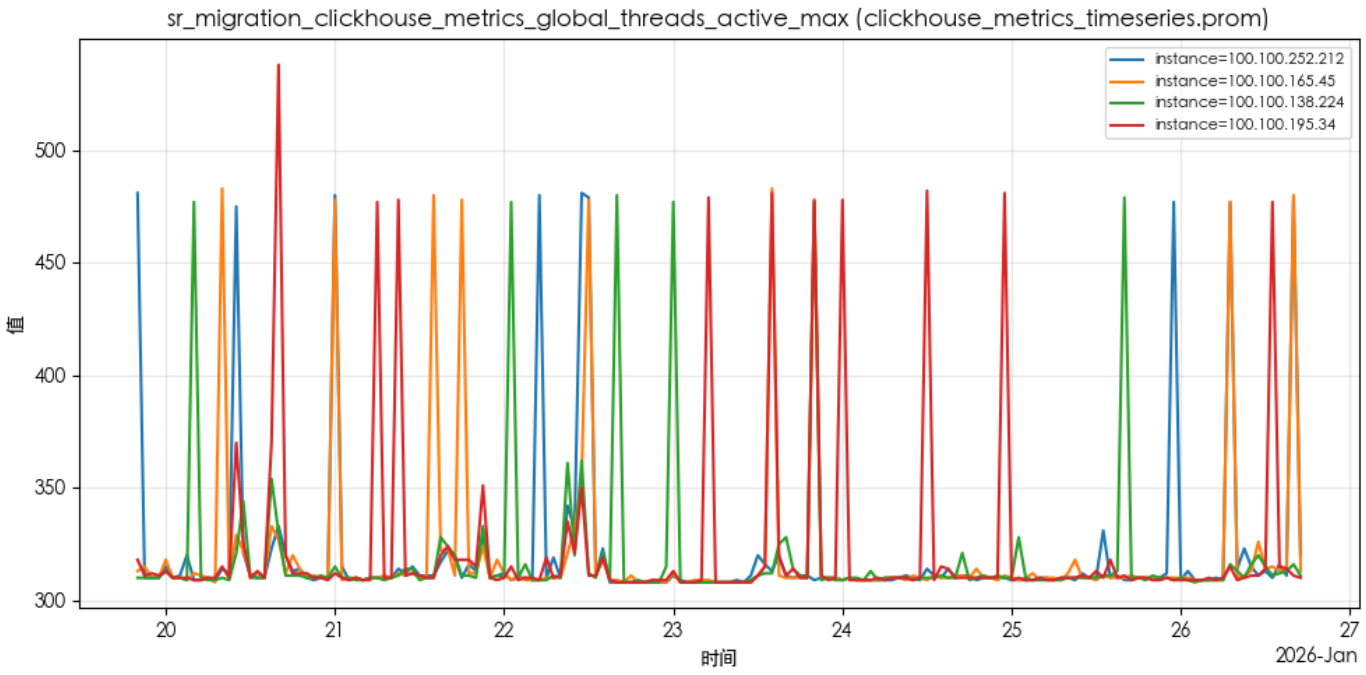
说明：正在执行查询数平均值，反映查询并发水平。



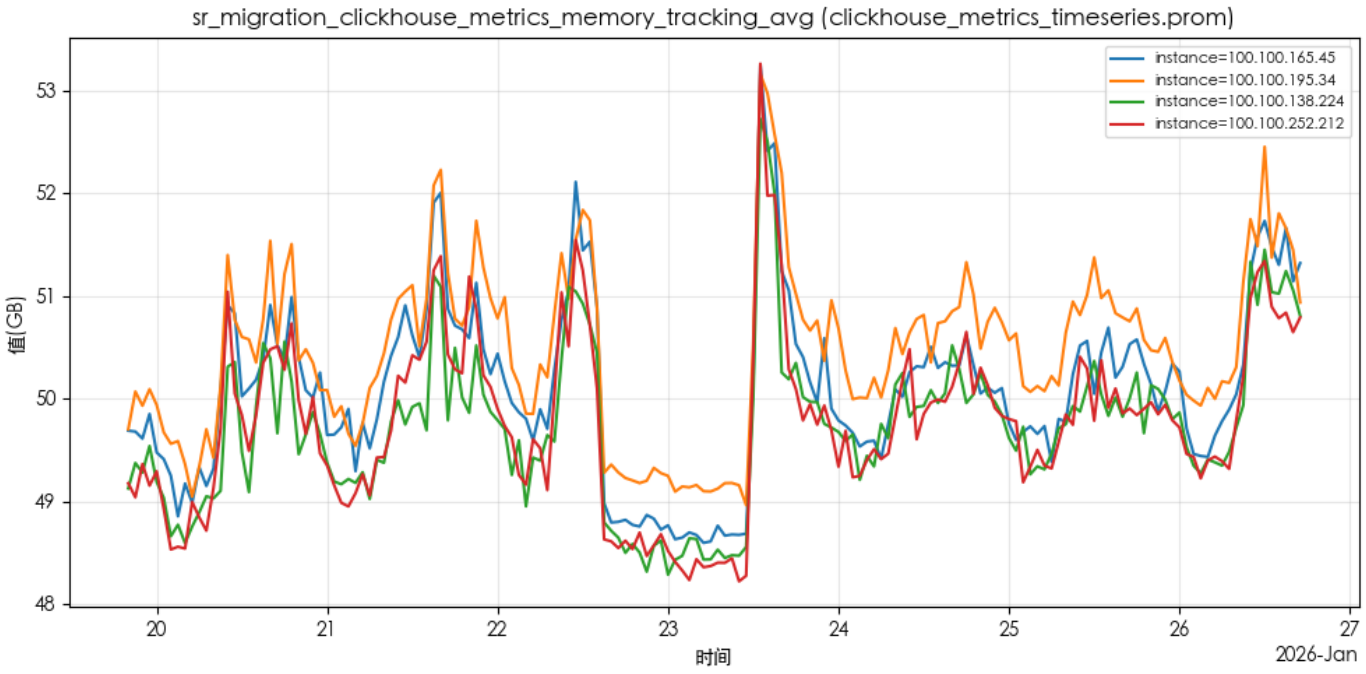
说明：正在执行查询数峰值，用于识别并发高峰。



说明：活跃线程数平均值，反映整体执行负载。

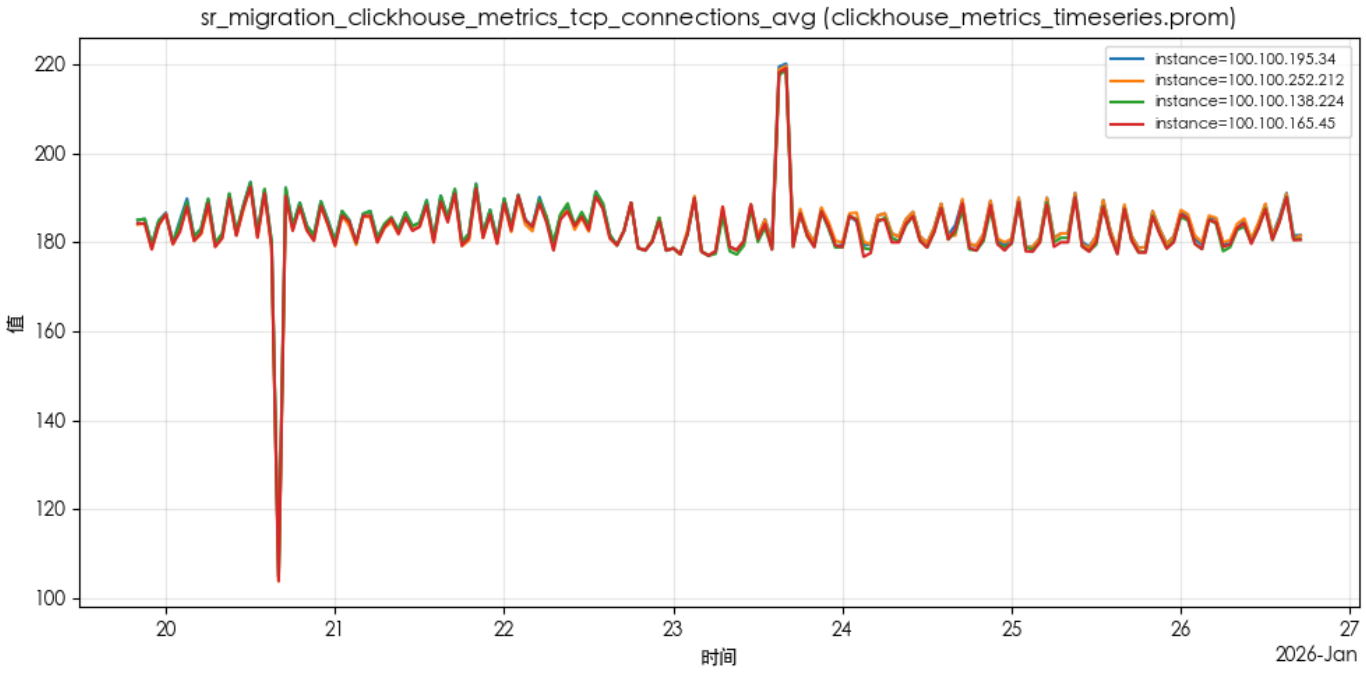


说明：活跃线程数峰值，用于识别线程高峰。

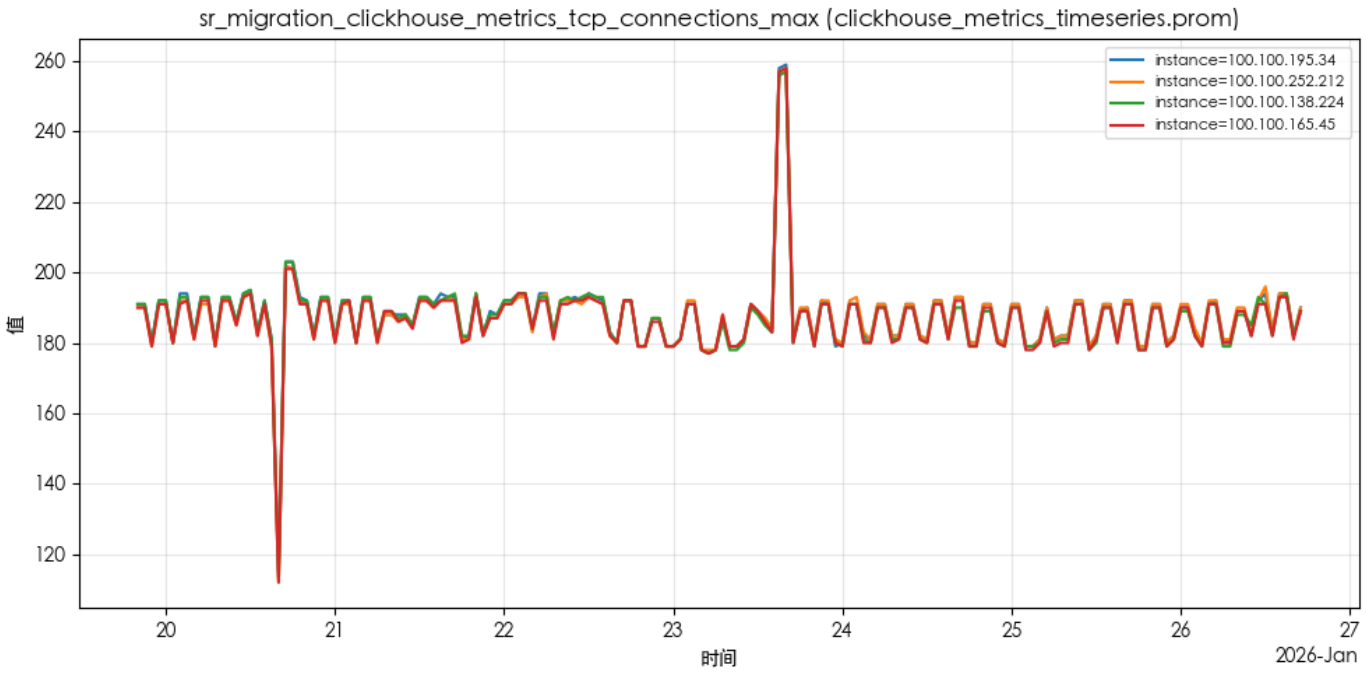


说明：ClickHouse内存跟踪值平均（(GB)），用于评估进程内存占用。

说明：ClickHouse内存跟踪值峰值（(GB)），用于识别内存尖峰。



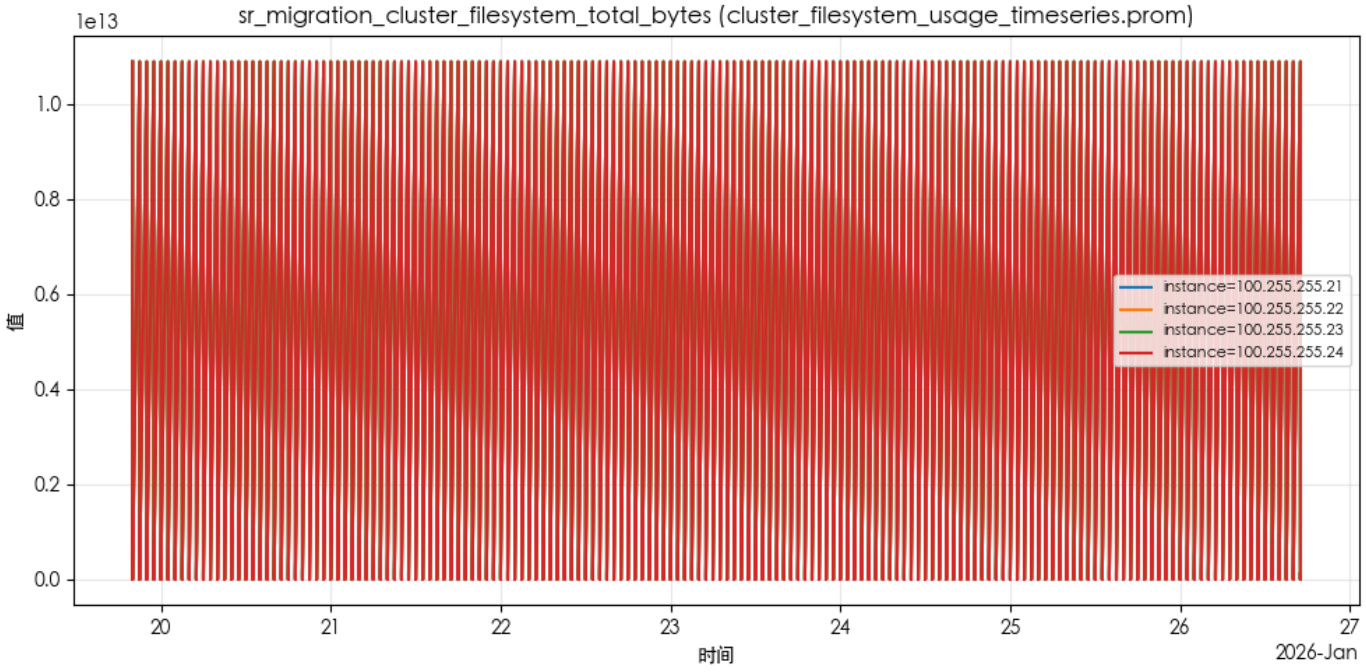
说明：TCP连接数平均值，反映客户端连接规模。



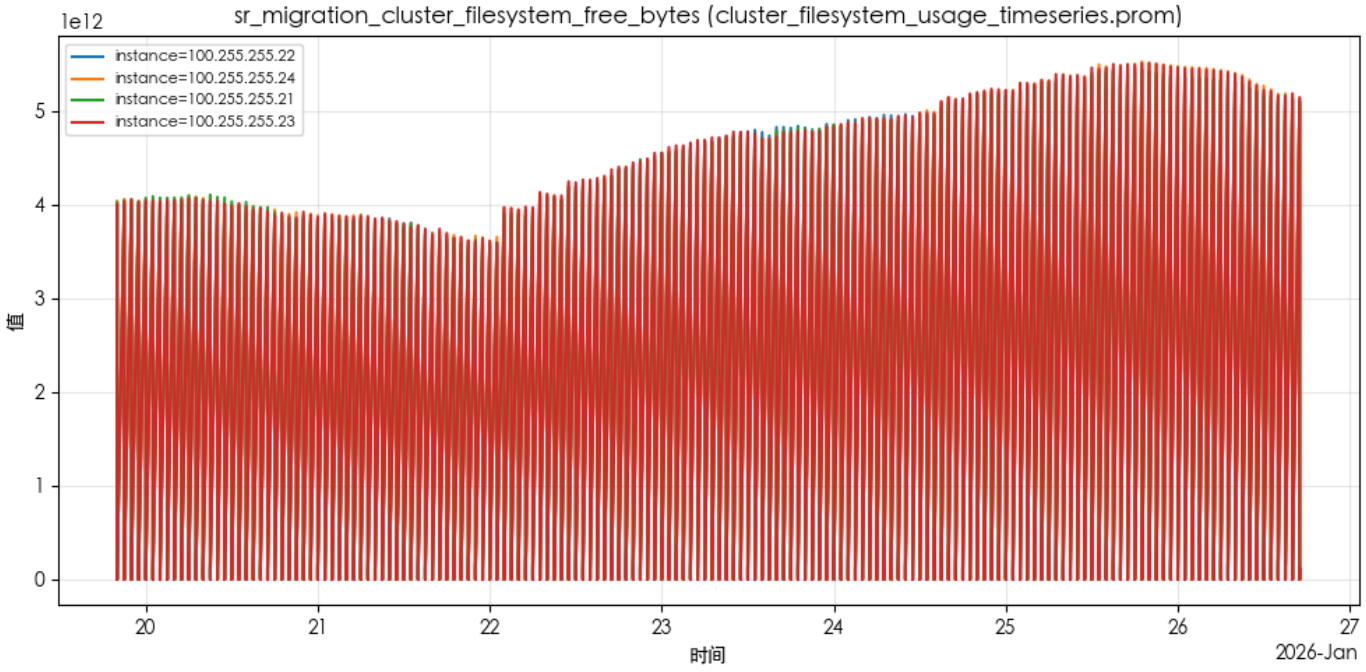
说明：TCP连接数峰值，用于识别连接突增。

节点文件系统

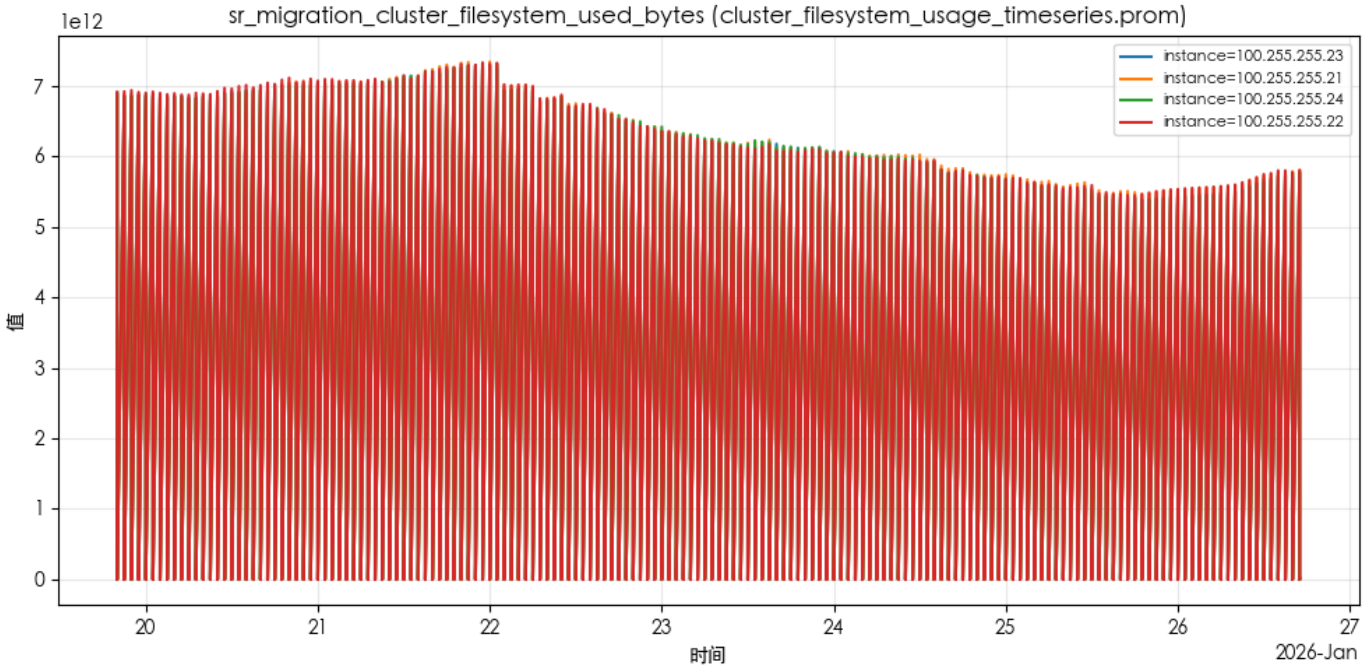
说明：展示节点文件系统容量与使用情况的变化趋势。



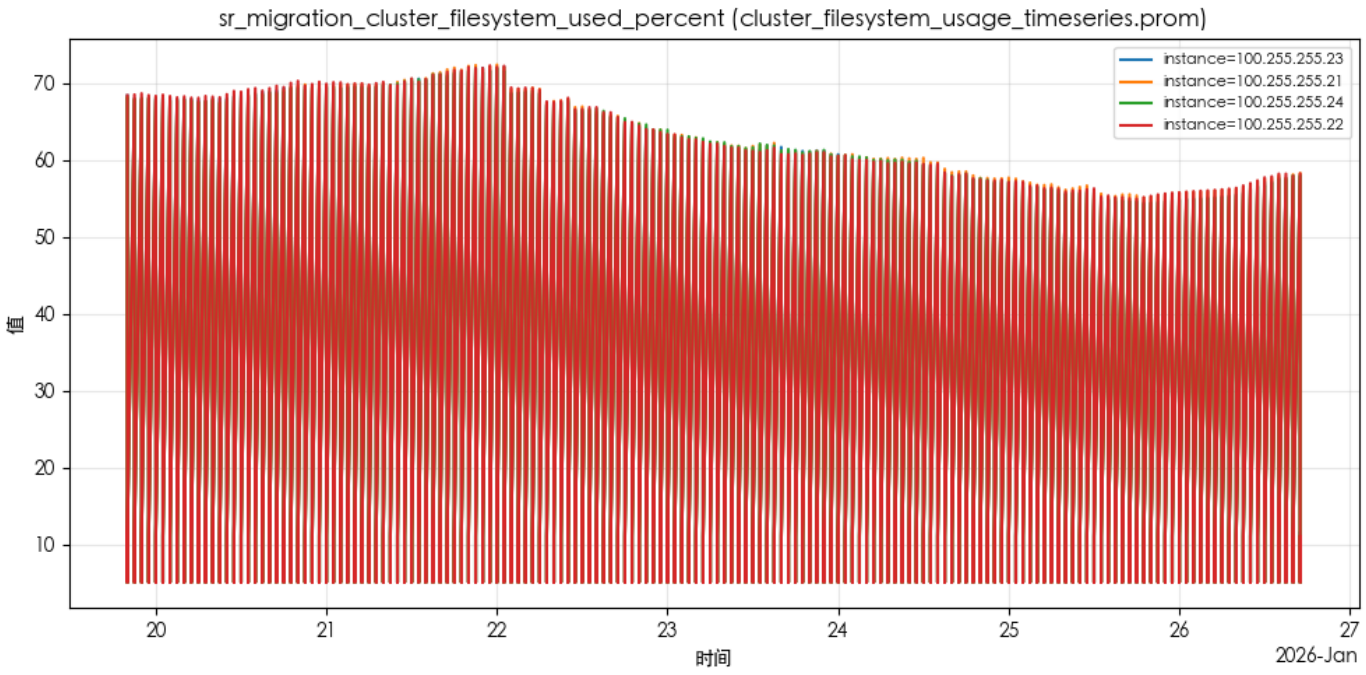
说明：文件系统总容量（GB），用于核对磁盘规模与规划。



说明：文件系统可用容量（GB），用于评估剩余空间。



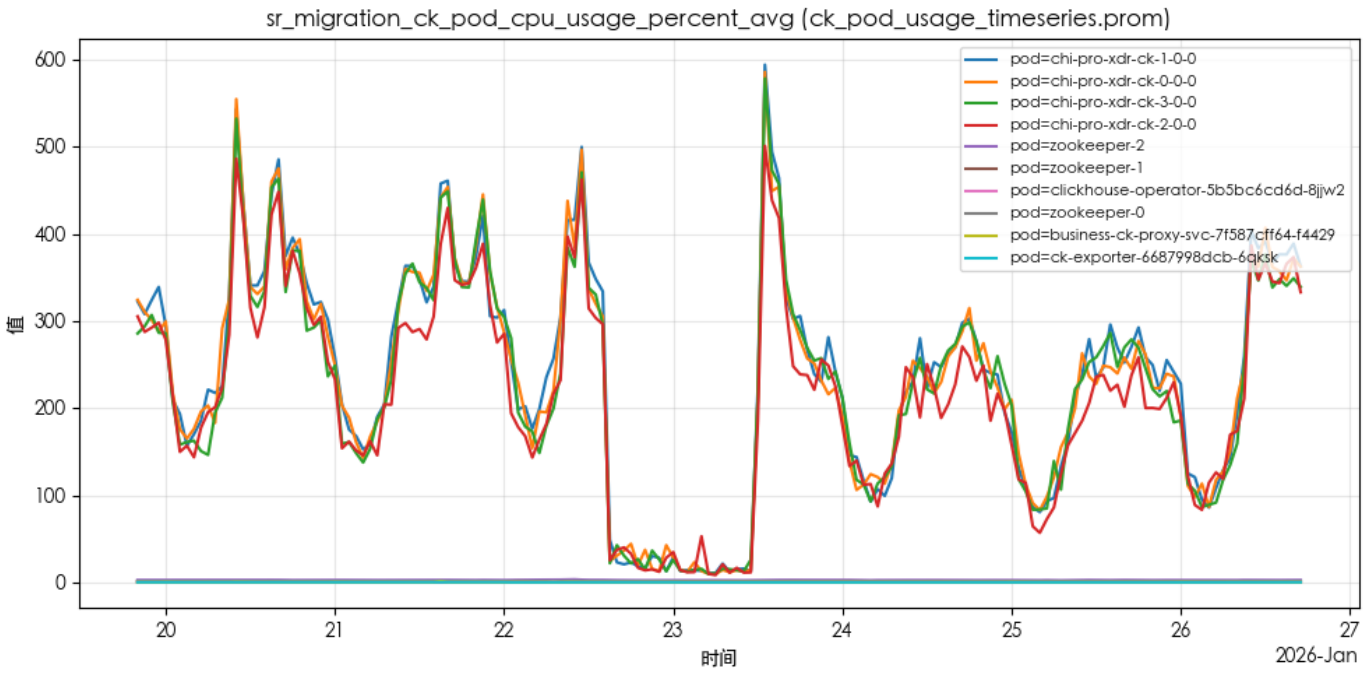
说明：文件系统已用容量（GB），用于观察容量增长趋势。



说明：文件系统使用率（%），用于识别空间紧张挂载点。

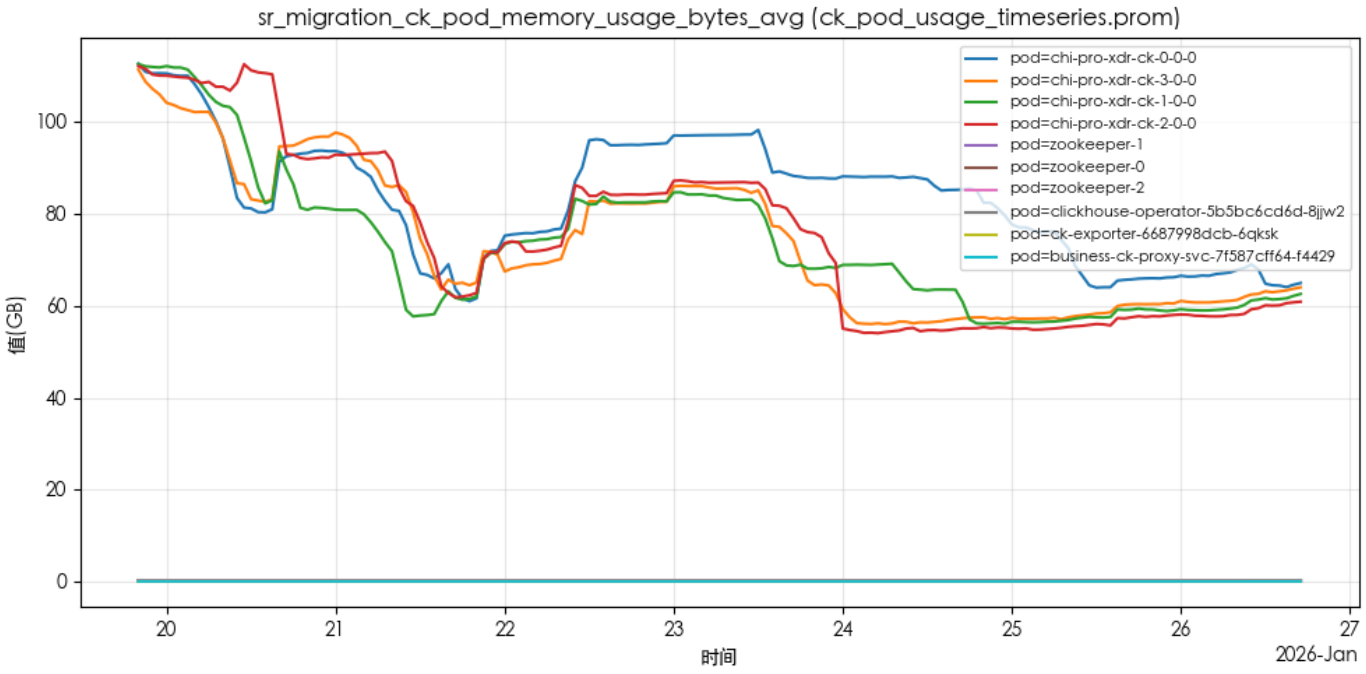
CK Pod资源

说明：展示CK Pod级别的资源使用情况与波动。

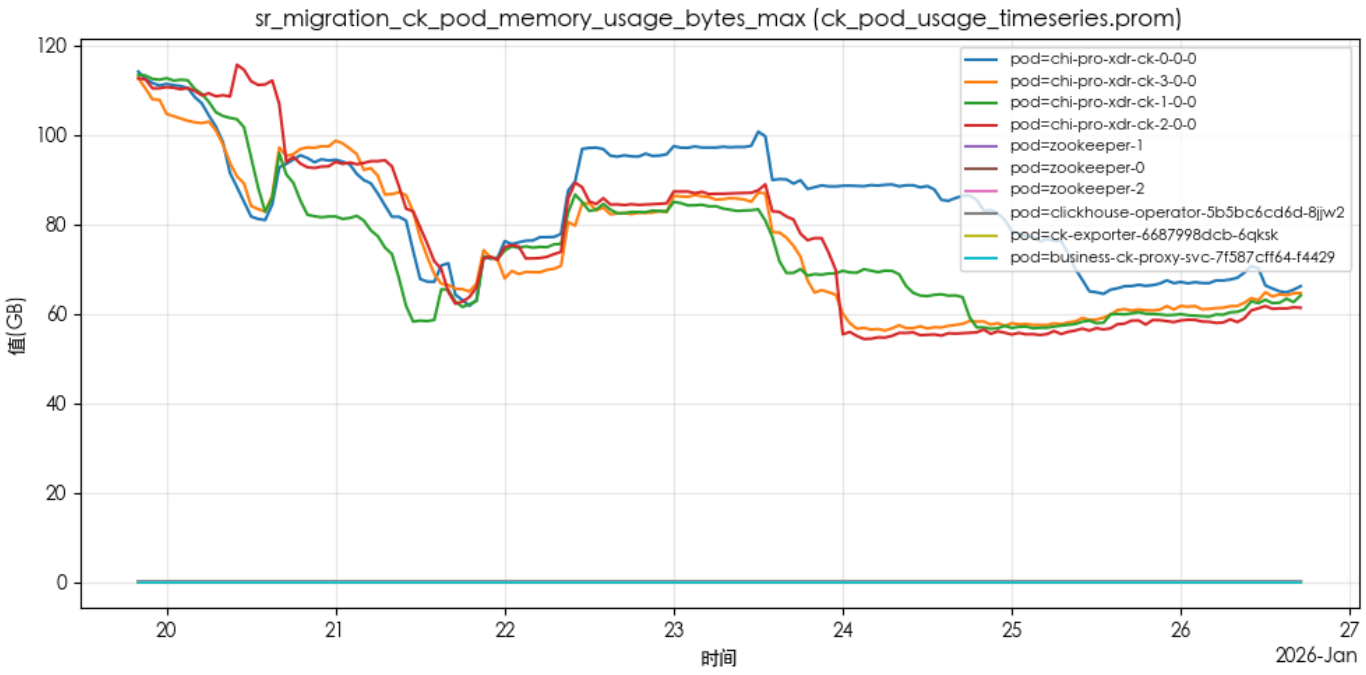


说明：CK Pod CPU使用率平均值，用于观察Pod计算负载。

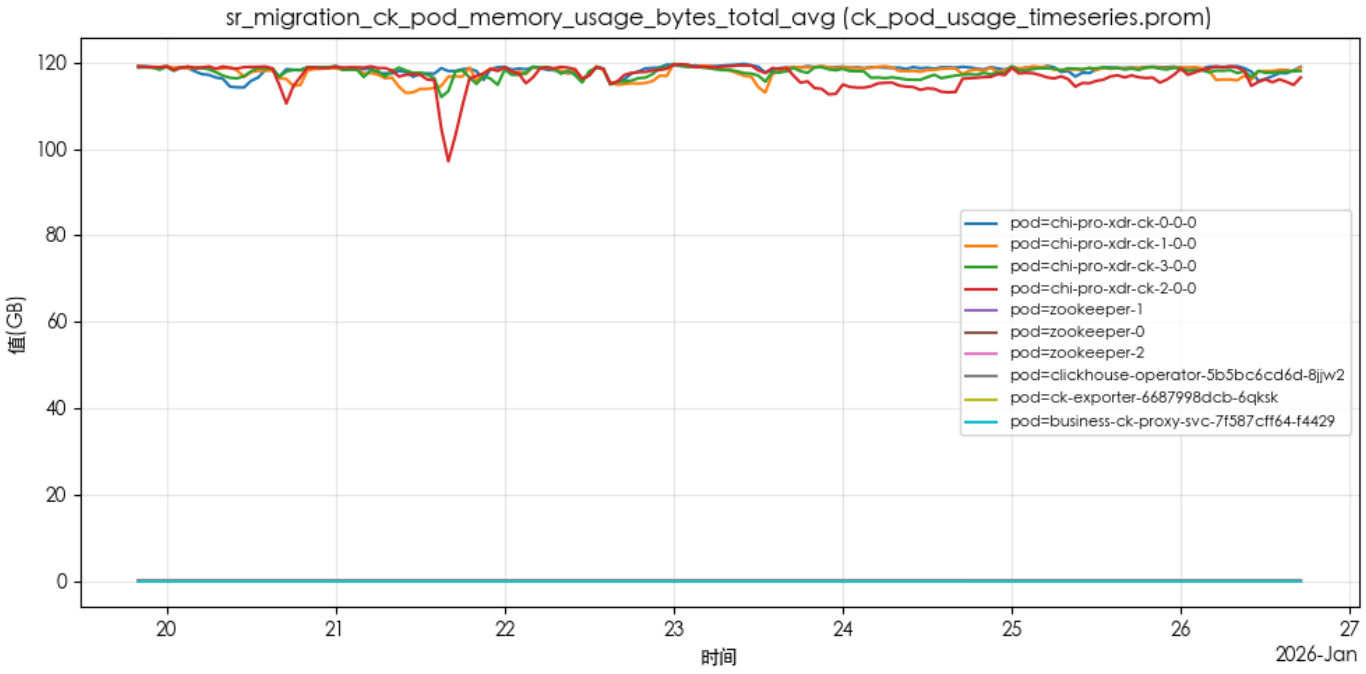
说明：CK Pod CPU使用率峰值，用于识别Pod CPU尖峰。



说明：CK Pod内存Working Set平均值（(GB)），用于观察实际活跃内存占用。

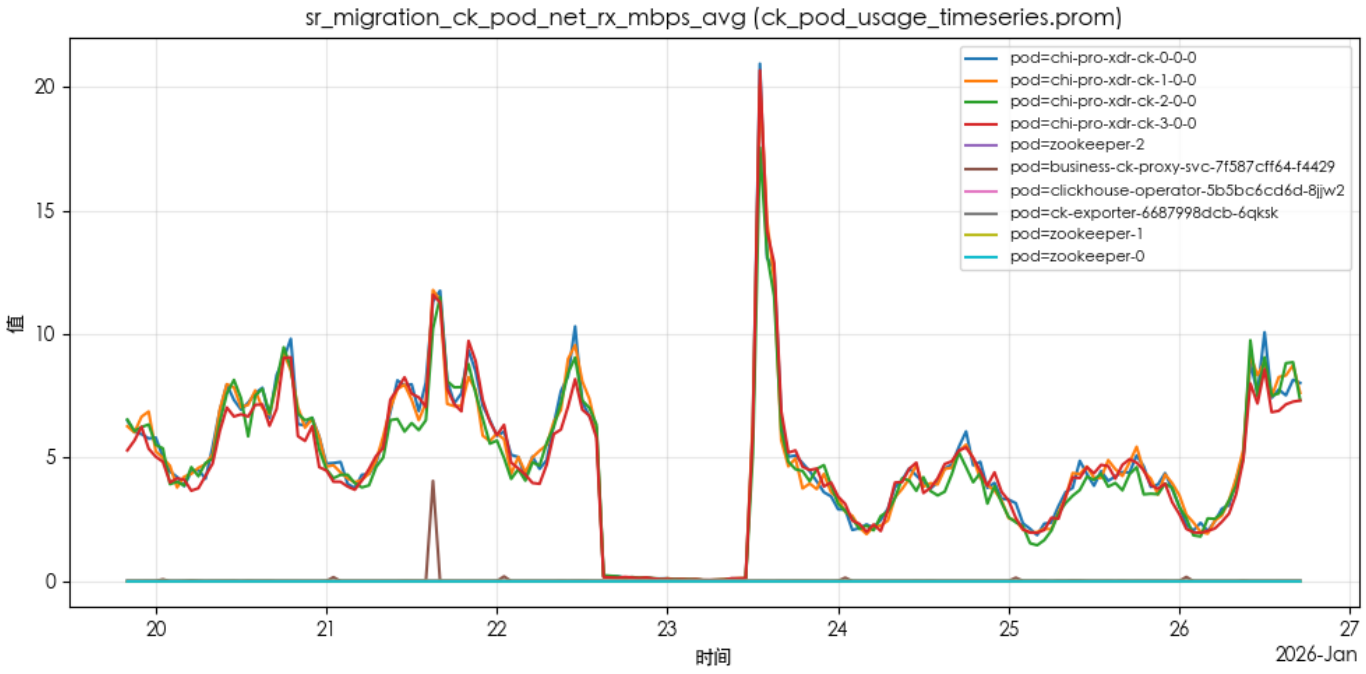


说明：CK Pod内存Working Set峰值（(GB)），用于识别内存尖峰。

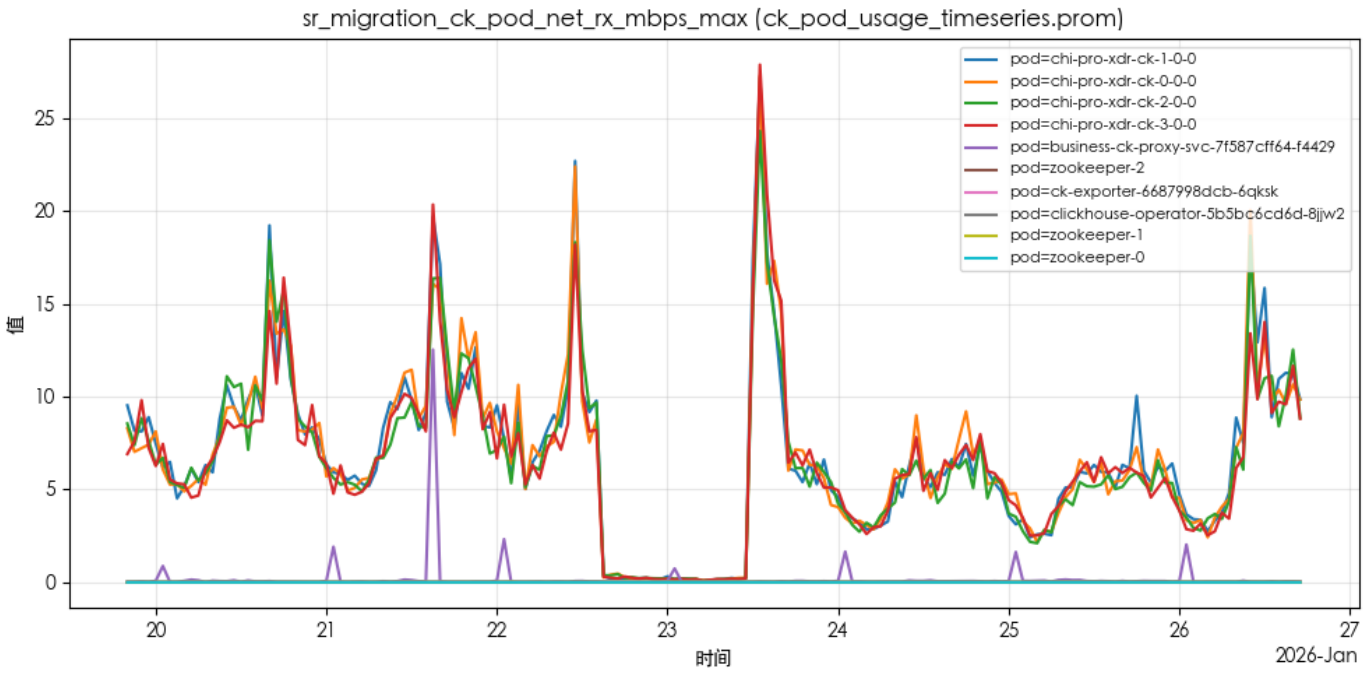


说明：CK Pod内存使用量平均值（(GB)，包含缓存），用于评估内存压力。

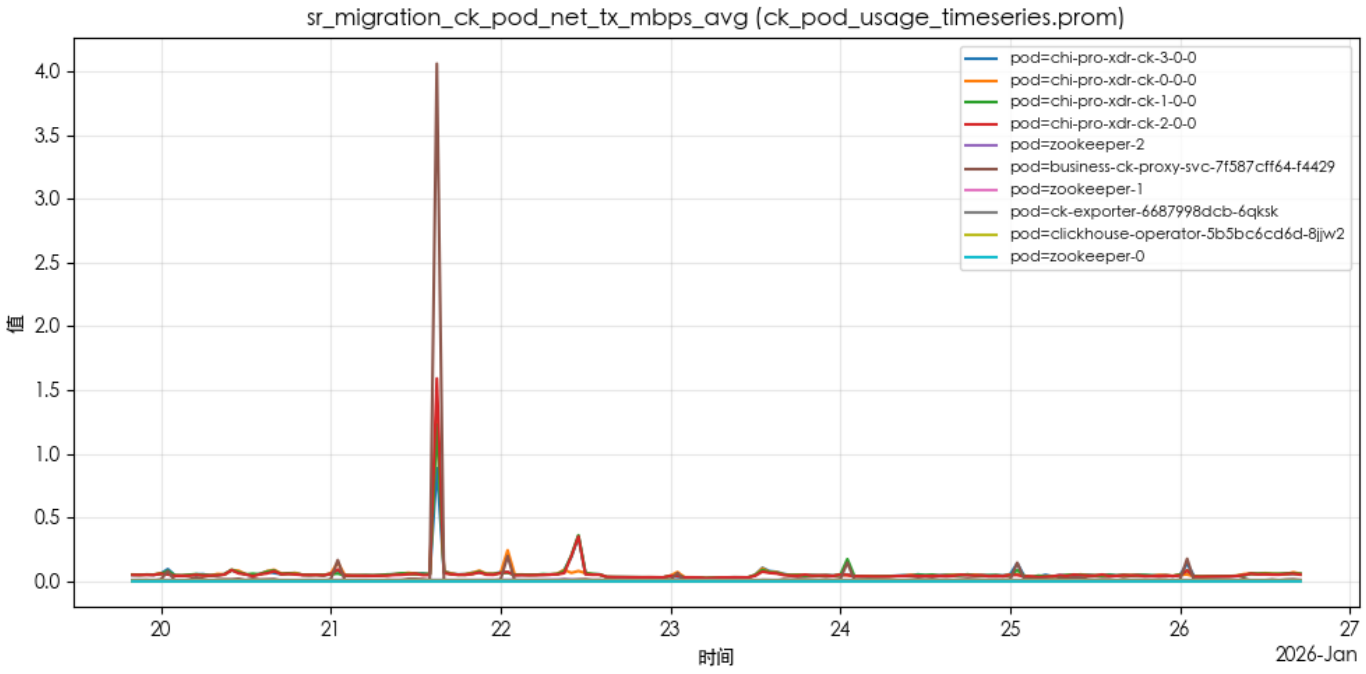
说明：CK Pod内存使用量峰值（(GB)，包含缓存），用于识别内存峰值。



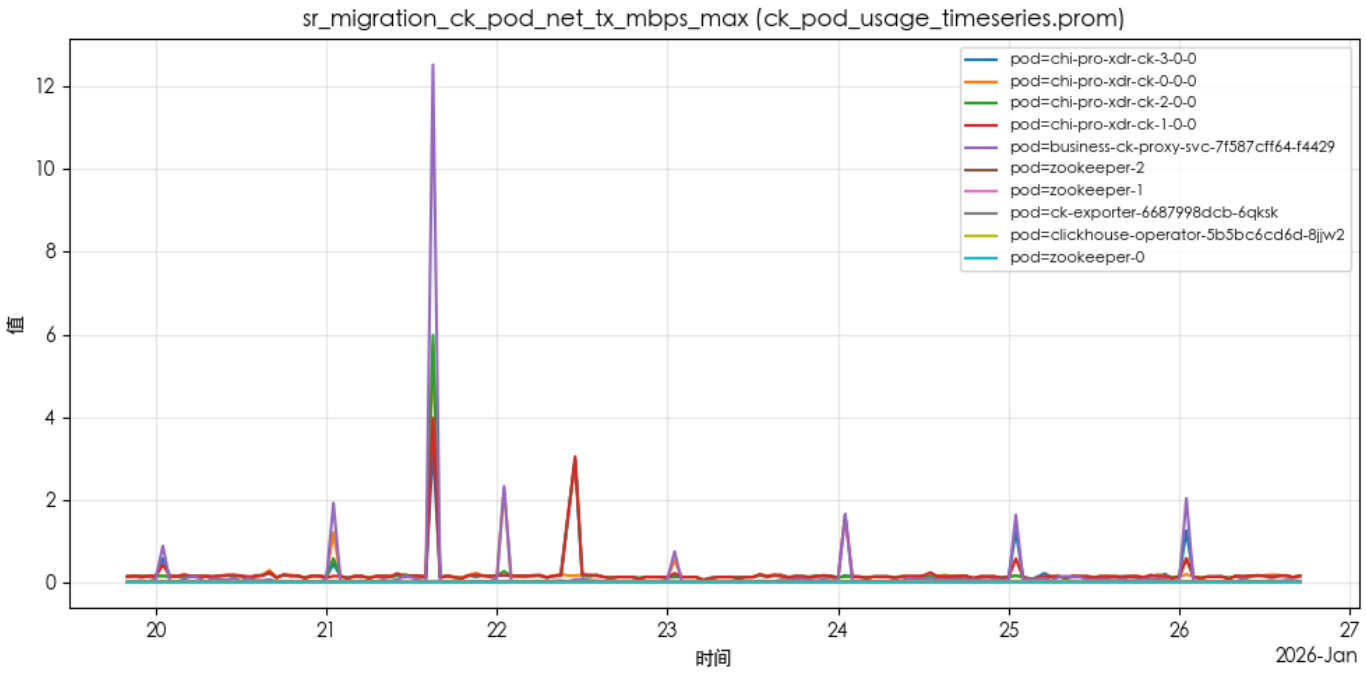
说明：CK Pod网络接收速率平均值（MB/s），反映入站带宽使用。



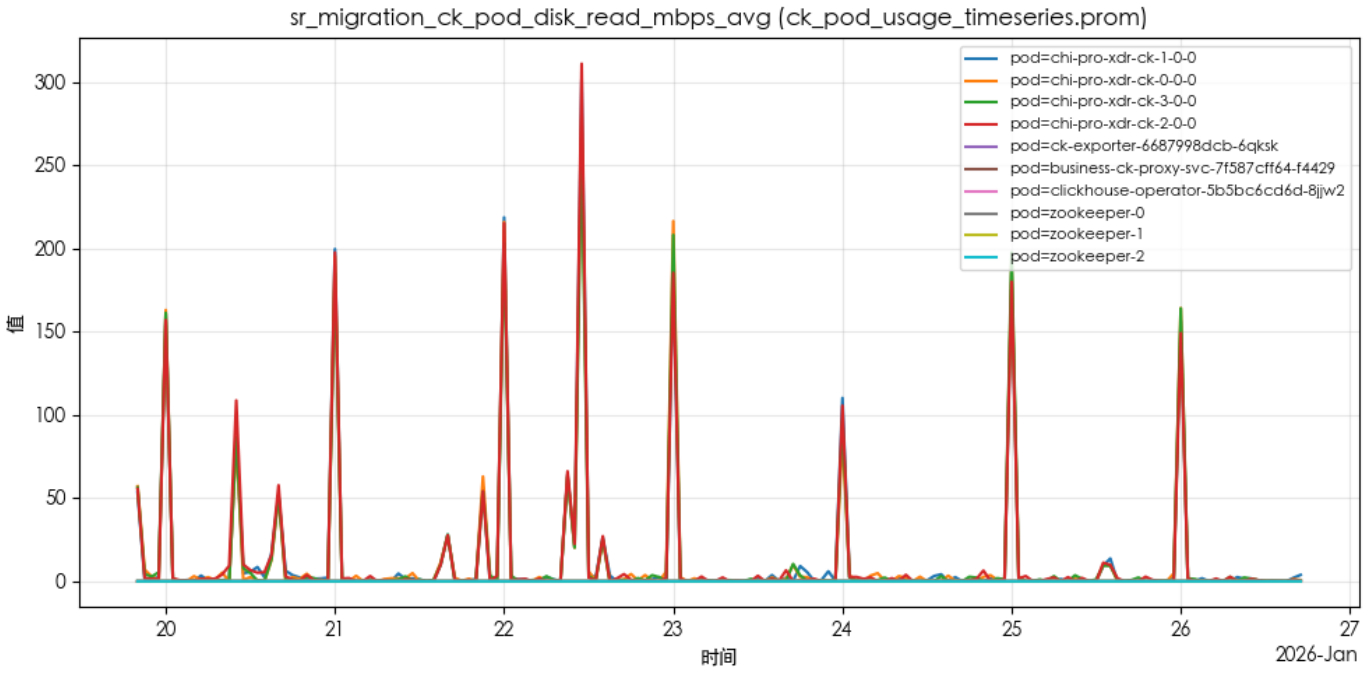
说明：CK Pod网络接收速率峰值（MB/s），用于识别入站突发流量。



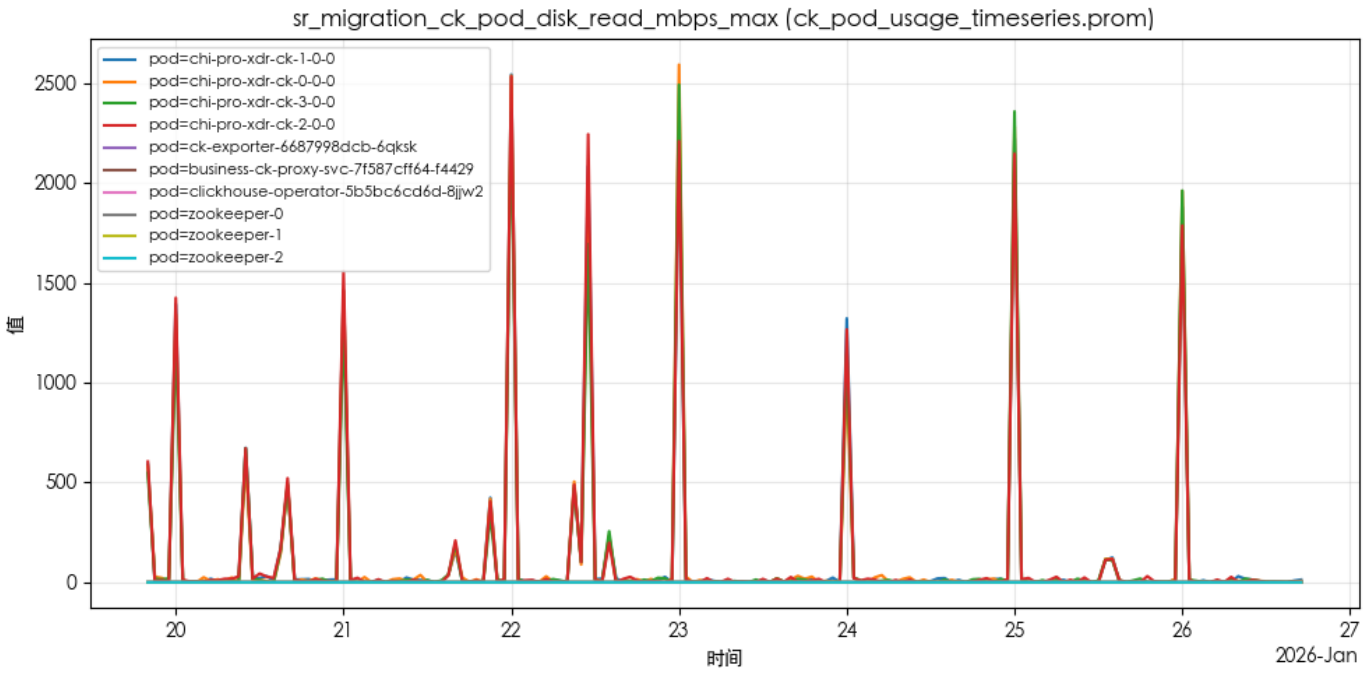
说明：CK Pod网络发送速率平均值（MB/s），反映出站带宽使用。



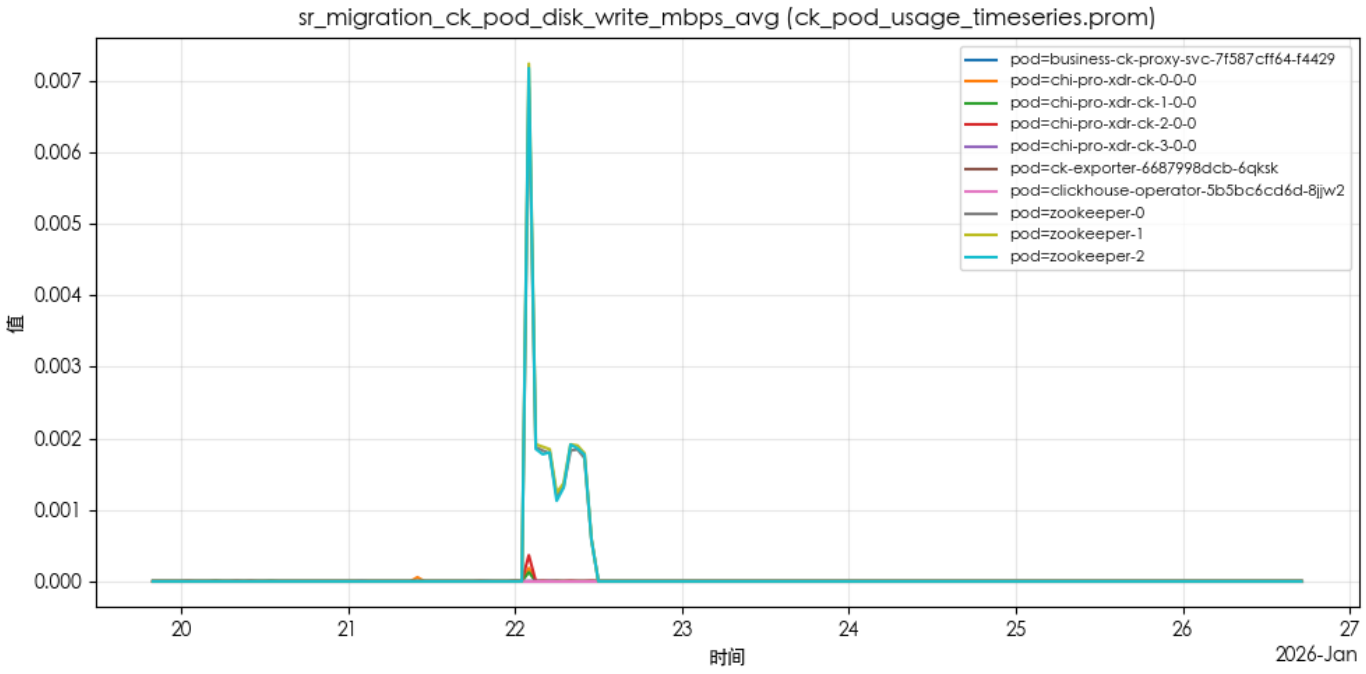
说明：CK Pod网络发送速率峰值（MB/s），用于识别出站突发流量。



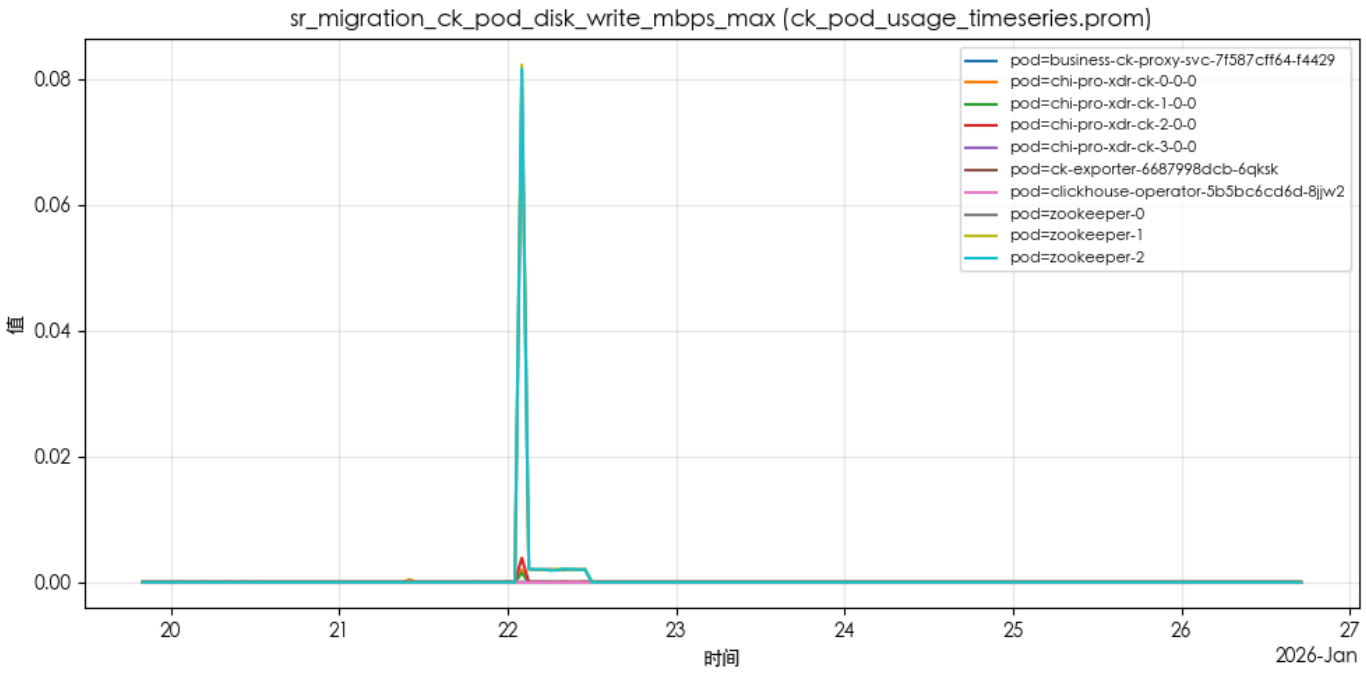
说明：CK Pod磁盘读速率平均值（MB/s），反映磁盘读吞吐。



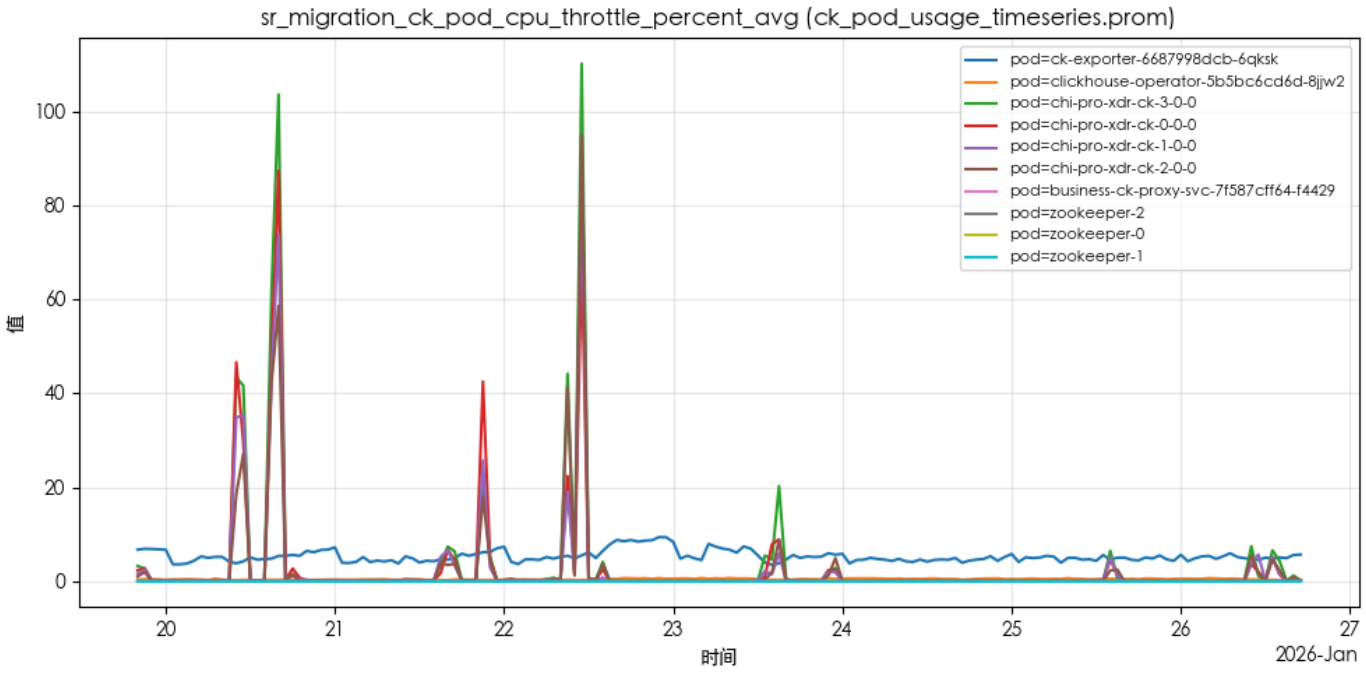
说明：CK Pod磁盘读速率峰值（MB/s），用于识别读突发。



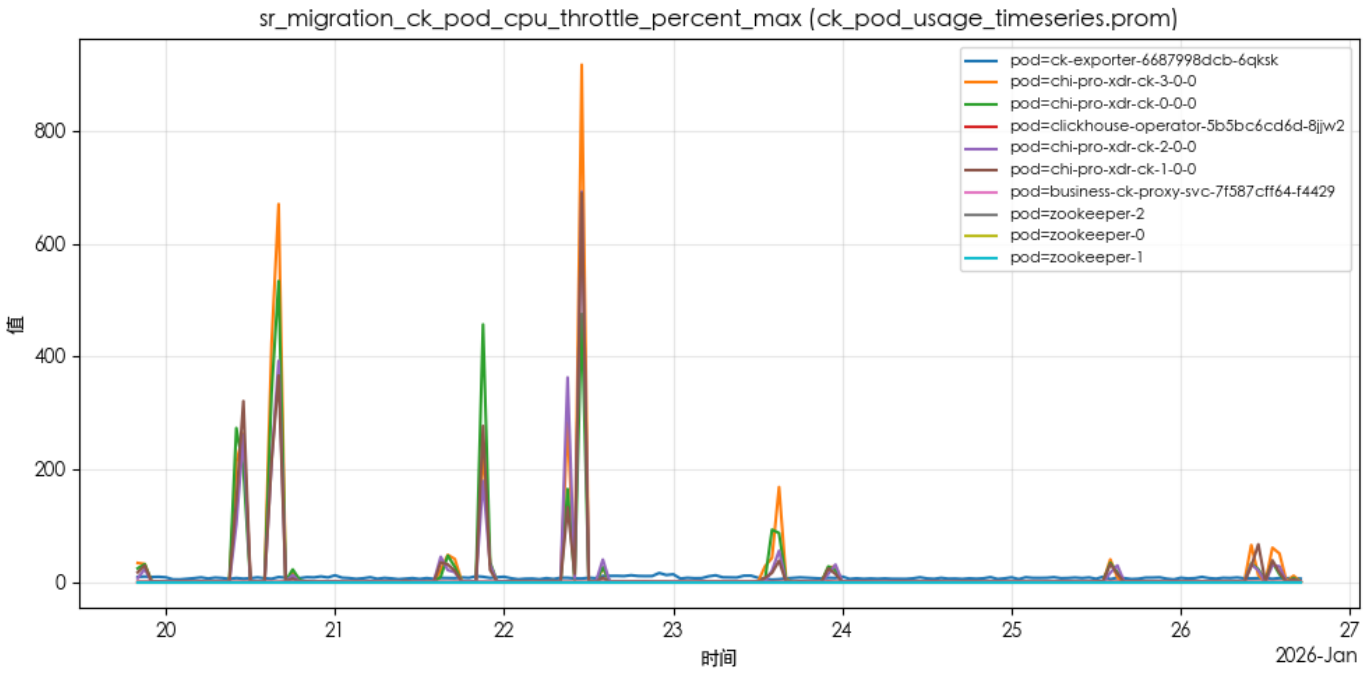
说明：CK Pod磁盘写速率平均值（MB/s），反映磁盘写吞吐。



说明：CK Pod磁盘写速率峰值（MB/s），用于识别写突发。



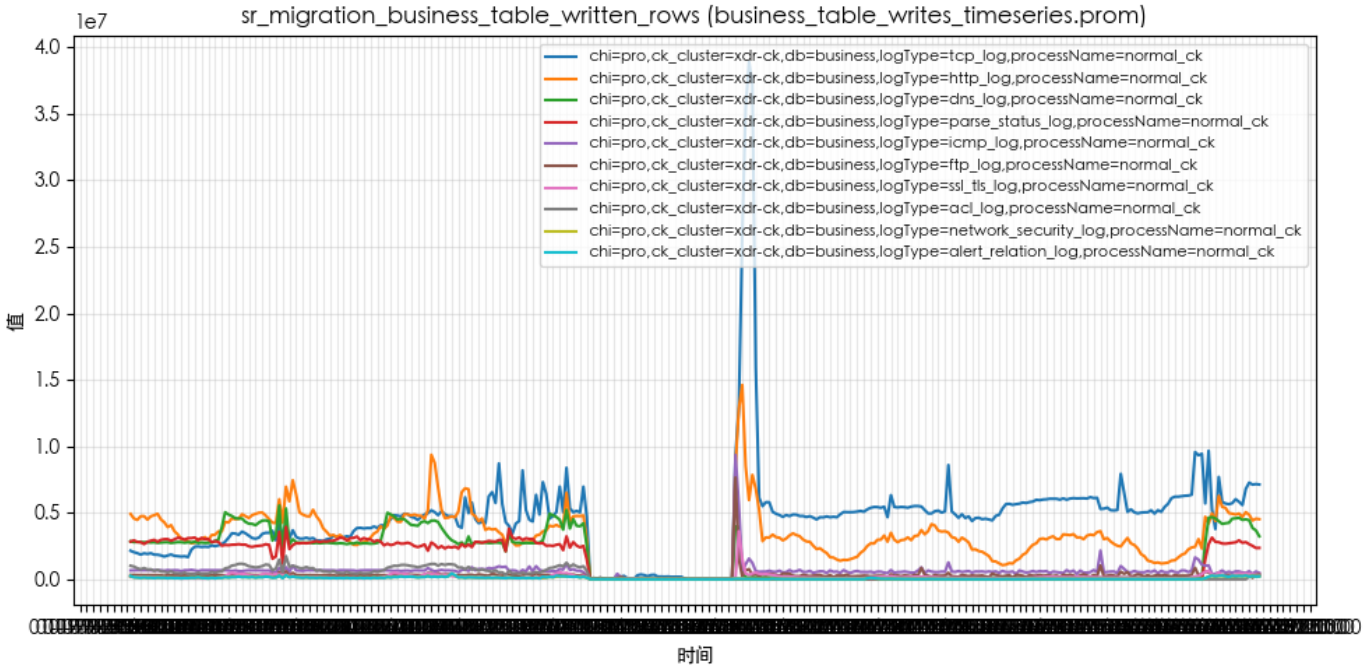
说明：CK Pod CPU节流占比平均值，反映CPU限额造成的节流程度。



说明：CK Pod CPU节流占比峰值，用于识别突发节流。

业务表写入

说明：展示业务表写入量随时间的变化趋势。



说明：业务表写入行数（按logType聚合），反映各业务日志类型的写入量变化。