

Warnmeldungen des Echtzeit-Überwachungstools

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[RTMT-Warnungen](#)

[Konfigurieren](#)

[Systemwarnungen](#)

[CallManager-Warnungen](#)

[LowAvailableVirtualMemory und LowSwapPartitionAvailableDiskSpace](#)

[LogPartitionHighWaterMarkExceeded und LogPartitionLowWaterMarkExceeded](#)

[CPU-Pegging](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument werden Warnungen des Cisco Real-Time Monitoring Tool (RTMT) behandelt und die Fehlerbehebung für einige häufig verwendete Warnungen erläutert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse der Cisco Call Manager-Webadministration zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco CallManager Server 11.0.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Das RTMT, das als clientseitige Anwendung ausgeführt wird, verwendet HTTPS und TCP, um die Systemleistung, den Gerätestatus, die Geräteerkennung, Computer Telephony Integration (CTI)-

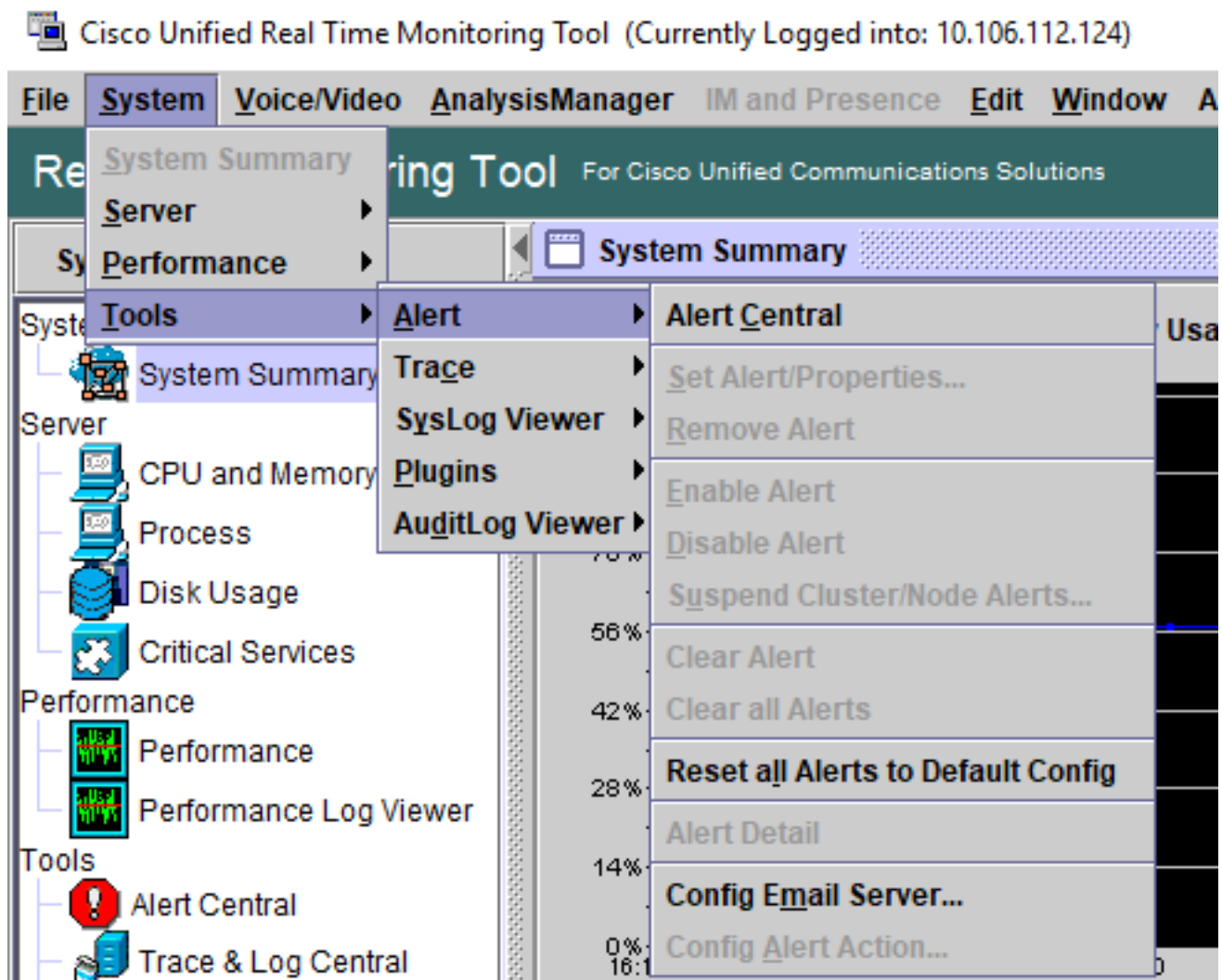
Anwendungen und Voice Messaging-Ports zu überwachen. RTMT kann verwendet werden, um Warnungen für den von ihm überwachten Cluster zu konfigurieren.

Das System generiert Warnmeldungen, um den Administrator zu benachrichtigen, wenn eine vordefinierte Bedingung erfüllt ist, z. B. wenn ein aktivierter Dienst deaktiviert wird. Das System kann Warnungen als E-Mail/E-Mail senden.

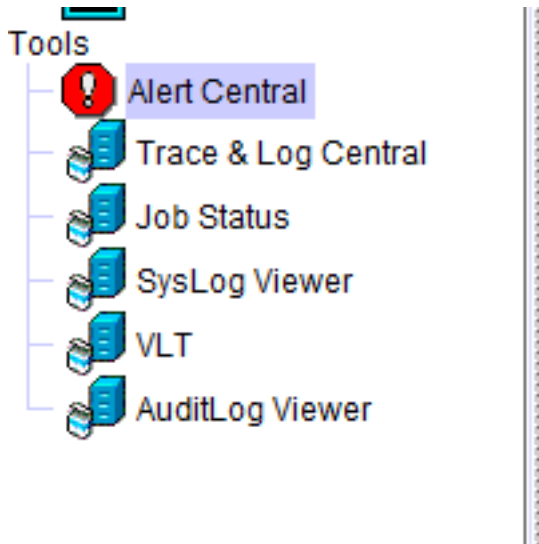
RTMT unterstützt das Definieren, Festlegen und Anzeigen von Warnmeldungen und enthält vorkonfigurierte und benutzerdefinierte Warnungen. Obwohl Sie Konfigurationsaufgaben für beide Typen durchführen können, können Sie vorkonfigurierte Warnungen nicht löschen.

RTMT-Warnungen

Das Unified RTMT zeigt sowohl vorkonfigurierte Warnungen als auch benutzerdefinierte Warnungen in Alert Central an, wie im Bild gezeigt.



Sie können auch auf Alert Central zugreifen, indem Sie im Systembereich in der Hierarchiestruktur auf das Symbol Alert Central klicken.



Konfigurieren

Das Unified RTMT organisiert die Warnungen unter den entsprechenden Registerkarten: System, CallManager, Cisco Unity Connection und Custom.

Alert Name	Enabled
ILSPwdAuthenticationFailed	Enabled
ILSTLSAuthenticationFailed	Enabled
IMEDistributedCacheInactive	Enabled
IMEOverQuota	Enabled
IMEQualityAlert	Enabled
IMEServiceStatus	Enabled
InsufficientFallbackIdentifiers	Enabled
InvalidCredentials	Enabled
LocationOutOfResource	Enabled
MaliciousCallTrace	Enabled

Sie können vorkonfigurierte und benutzerdefinierte Warnungen in Alert Central aktivieren oder deaktivieren. Sie können jedoch vorkonfigurierte Warnungen nicht löschen.

DBReplicationFailure	Enabled	Yes
DBReplicationTableOutOfSync	Enabled	N/A
HardwareFailure	Enabled	N/A
LogFileSearchStringFound	Enabled	N/A
LogPartitionHighWaterMarkExceeded	Enabled	N/A
LogPartitionLowWaterMarkExceeded	Enabled	N/A
LowActivePartitionAvailableDiskSpace	Enabled	Yes
LowAvailableVirtualMemory	Enabled	Yes
LowInactivePartitionAvailableDiskSpace	Enabled	Yes
LowSwapPartitionAvailableDiskSpace	Enabled	Yes
ServerDown	Enabled	Yes
SparePartitionHighWaterMarkExceeded	Enabled	N/A
SparePartitionLowWaterMarkExceeded	Enabled	N/A
SyslogSeverityMatchFound	Enabled	N/A
SyslogStringMatchFound	Enabled	N/A
SystemVersionMismatched	Enabled	Yes
TotalProcessesAndThreadsExceededThreshold	Enabled	Yes

Warnungen in RTMT werden wie folgt klassifiziert:

- [Systemwarnungen](#)
- [CallManager-Warnungen](#)
- Benutzerdefinierte Alarme

Systemwarnungen

Diese Liste enthält vorkonfigurierte Systemwarnungen:

- Authentifizierung fehlgeschlagen
- CiscoDRFleise
- CoreDumpFileFound
- CPU-Pegging
- CriticalAuditEventGenerated
- CriticalServiceDown
- Hardware-Fehler
- LogFileSearchStringFound
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- LowActivePartitionAvailableDiskSpace
- Gering verfügbarer virtueller Arbeitsspeicher
- LowInactivePartitionAvailableDiskSpace
- LowSwapPartitionAvailableDiskSpace
- ServerDown (gilt für Unified Communications Manager (CUCM)-Cluster)

- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- SystemVersionMismatch
- TotalProcessesAndThreadsOverceededThreshold

CallManager-Warnungen

Diese Liste enthält die vorkonfigurierten CallManager-Warnungen.

- BeginThrottlingCallListBLFS-Abonnements
- CallAttemptBlockedByPolicy
- CallProcessingNodeCPUpegging
- CARIDSEngineCritical
- CARIDSEngineFailure
- CARSplanerJobFailed
- CDRAgentSendFileFailed
- CDRFileDelivery fehlgeschlagen
- CDRHighWaterMarkExceeded
- CDRMaximumDiskSpaceExceeded
- CodeYellow
- DBChangeNotifyFailure
- DBReplicationFailure
- DBReplicationTableOutOfSync
- DDRBlockPrevention
- DDRDown
- EMCCFailInLocalCluster
- EMCCFailInRemoteCluster
- ExcessiveVoiceQualityReports
- IMEDistributedCacheInaktiv
- IMEOverQuote
- IMEQualityAlert
- UngenügendFallbackIdentifiers
- IMEServiceStatus
- InvalidCredentials
- LowTFTPServerHeartbeatRate
- MaliciousCallTrace
- MediaListExhausted
- MgcDChannelOutOfService
- Anzahl der registrierten GeräteÜbersprungen
- Anzahl der registrierten GatewaysVermindert
- Anzahl der registrierten GatewaysErhöht
- Anzahl der registrierten MediengeräteVermindert
- Anzahl der registrierten MediengeräteErhöhte Anzahl

- Anzahl der registrierten TelefoneVerworfen
- RouteListExhausted
- SDLWinkOutOfService
- TCPSetupToIMEFail
- TLSConnectionToIMEFail
- UserInputFailure

LowAvailableVirtualMemory und LowSwapPartitionAvailableDiskSpace

Linux-Server neigen dazu, die Auslastung des virtuellen Speichers über einen bestimmten Zeitraum zu "unklar" zu machen, und es hat sich gezeigt, dass sich diese Warnungen häufen und daher auch diese Warnmeldungen.

```
LowActivePartitionAvailableDiskSpace
LowAvailableVirtualMemory
LowInactivePartitionAvailableDiskSpace
LowSwapPartitionAvailableDiskSpace
ServerDown
```

Linux arbeitet etwas anders als ein Betriebssystem.

Nachdem der Speicher einem Prozess zugewiesen wurde, wird er vom Prozessor nur dann zurückgenommen, wenn ein anderer Prozess mehr Speicher als den verfügbaren Speicher anfordert.

Dies verursacht einen hohen virtuellen Speicher.

Ein Antrag auf Erhöhung des Schwellenwerts für den Alarm in den höheren Versionen des Call Managers ist im Fehler dokumentiert:

https://bst.cloudapps.cisco.com/bugsearch/bug/CSCuq75767/?referring_site=dumpcr

Bei Swap-Partitionen zeigt diese Warnung an, dass die Swap-Partition nicht über genügend Speicherplatz verfügt und vom System stark genutzt wird. Die Swap-Partition wird normalerweise verwendet, um die physische RAM-Kapazität bei Bedarf zu erweitern. Wenn der RAM ausreichend ist, sollte unter normalen Bedingungen der Austausch nicht zu viel verwendet werden.

Diese können auch RTMT-Warnungen auslösen, die durch das Erstellen von Temp-Dateien verursacht werden. Es wird empfohlen, den Server neu zu starten, um unnötige Temp-Dateien zu löschen.

LogPartitionHighWaterMarkExceeded und LogPartitionLowWaterMarkExceeded

Beim Ausführen des **Anzeigestatus** auf der CLI eines CUCM-Servers wird ein Wert angezeigt, der den besetzten und freien Prozentsatz der Protokollierungspartition im CUCM-Festplattenspeicher angibt. Diese Werte werden auch als gemeinsame Partition bezeichnet und geben den Speicherplatz an, der von den Protokollen/Ablaufverfolgungen und den CDR-Dateien im Server belegt ist. Diese Dateien sind zwar harmlos, können aber aufgrund des zeitlichen Speichermangels Probleme bei der Installation/Aktualisierung verursachen. Diese Warnmeldungen dienen als Warnung an den Administrator, die Protokolle zu löschen, die im Laufe der Zeit möglicherweise im Cluster/Server angesammelt wurden.

LogPartitionLowWaterMarkExceeded: Diese Warnung wird generiert, wenn der gefüllte Speicherplatz die für die Warnung konfigurierten Schwellenwerte erreicht. Diese Warnung dient als Vorabkontrollanzeige für die Festplattennutzung.

LogPartitionHighWaterMarkExceeded: Diese Warnung wird generiert, wenn der gefüllte Speicherplatz die für die Warnung konfigurierten Schwellenwerte erreicht. Sobald die Warnmeldung generiert wurde, löscht der Server automatisch die ältesten Protokolle, um den Speicherplatz auf Werte herabzusetzen, die dem HighWaterMark-Schwellenwert entsprechen.

Als Best Practice sollten die Protokolle manuell gelöscht werden, sobald die LogPartitionLowWaterMarkExceeded-Warnung empfangen wird.

Dies sind die folgenden Schritte:

Schritt 1: Starten Sie RTMT.

Schritt 2: Wählen Sie **Alert Central aus**, und führen Sie dann die folgenden Aufgaben aus:

Wählen Sie **LogPartitionHighWaterMarkExceeded aus**, notieren Sie den Wert und ändern Sie den Schwellenwert auf 60 %.

Wählen Sie **LogPartitionLowWaterMarkExceeded aus**, notieren Sie den Wert und ändern Sie den Schwellenwert auf 50 %.

Das Polling findet alle 5 Minuten statt. Warten Sie also 5-10 Minuten, und überprüfen Sie dann, ob der erforderliche Speicherplatz verfügbar ist. Wenn Sie mehr Speicherplatz in der gemeinsamen Partition freigeben möchten, ändern Sie die LogPartitionHighWaterMarkExceeded-Threadwerte und die LogPartitionLowWaterMarkExceeded-Werte wieder in niedrigere Werte (z. B. 30 % und 20 %).

Geben Sie ihm 15 bis 20 Minuten, um den Speicherplatz in der gemeinsamen Partition freizugeben. Sie können die Verringerung der Festplattenauslastung mit dem Befehl **show status** from CLI überwachen.

Das würde die gemeinsame Teilung zum Erliegen bringen.

CPU-Pegging

Der CpuPegging-Alarm überwacht die CPU-Auslastung anhand des konfigurierten Grenzwerts.

Wenn die CPU-Pegging-Warnung empfangen wird, kann der Prozess, der die höchste CPU belegt, über die Systemablage links, d. h. Prozess, ausgeführt werden.

Process	PID	% CPU	Status	Shared Memory (K)
tomcat#1	10084	3	SLEEPING	4552
RisDC	18351	1	SLEEPING	18368
async/mgr	26	0	SLEEPING	0
ata_sff/3	45	0	SLEEPING	0
ata_sff/2	44	0	SLEEPING	0
pciehpd	82	0	SLEEPING	0
ata_sff/1	43	0	SLEEPING	0
ata_sff/0	42	0	SLEEPING	0
startdiscrpt.	8545	0	SLEEPING	1020
jbd2/sda3-8	756	0	SLEEPING	0
sshd#2	8935	0	SLEEPING	404
cgroup	23	0	SLEEPING	0
sshd#1	8544	0	SLEEPING	864
jbd2/sda6-8	754	0	SLEEPING	0
cmoninit#20	25372	0	SLEEPING	7372
host_agent.pl	19199	0	SLEEPING	636

Aus der CLI des betreffenden Servers ergeben sich daraus einige Einblicke.

- **utils diagnose test**
- **show process load cpu sortiert**
- **Anzeigestatus**
- **utils Core Active List**

Es wird empfohlen zu beobachten, ob der CPU-Spitzenwert zu einem bestimmten Zeitpunkt oder zufällig auftritt. Wenn es willkürlich vorkommt, werden die erforderlichen detaillierten CUCM-Traces sowie RisDC-Parmon-Protokolle ausgeführt, um zu überprüfen, was die Spitze in der CPU auslöst. Wenn die Warnungen zu einer bestimmten Tageszeit erfolgen, könnte dies auf geplante Aktivitäten wie Disaster Recovery System (DRS) Backup, CDR Load usw. zurückzuführen sein.

Darüber hinaus werden anhand von Informationen darüber, welcher Prozess die meisten CPUs belegt, spezifische Protokolle für weitere Untersuchungen herangezogen. Beispiel: Wenn der Schuldige Tomcat ist, werden die Tomcat-bezogenen Protokolle benötigt.


```
admin:utils diagnose test

Log file: platform/log/diag3.log

Starting diagnostic test(s)
=====
test - disk_space      : Passed (available: 1160 MB, used: 12522 MB)
skip - disk_files      : This module must be run directly and off hours
test - service_manager : Passed
test - tomcat           : Passed
test - tomcat_deadlocks : Passed
test - tomcat_keystore  : Passed
test - tomcat_connectors : Passed
test - tomcat_threads   : Passed
test - tomcat_memory    : Failed - Tomcat's memory usage is unusually high.
Use the 'utils diagnose module tomcat_heapdump' command to generate a memory dump
for further analysis. Note, creating the memory dump will increase CPU usage
and disk I/O for several minutes. Web services will also be disabled while the
memory dump is generated.
test - tomcat_sessions  : Passed
skip - tomcat_heapdump  : This module must be run directly and off hours
test - validate_network : Passed
test - raid              : Passed
test - system_info      : Passed (Collected system information in diagnostic
log)
test - ntp_reachability  : Passed
test - ntp_clock_drift  : Passed
test - ntp_stratum       : Passed
skip - sdl_fragmentation : This module must be run directly and off hours
skip - sdi_fragmentation : This module must be run directly and off hours

Diagnostics Completed

The final output will be in Log file: platform/log/diag3.log

Please use 'file view activelog platform/log/diag3.log' command to see the output
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Wenn die Warnungen nicht gelöscht werden, nachdem Sie die hier vorgeschlagenen Problemumgehungen befolgt haben oder die Warnungen unmittelbare Auswirkungen auf den Service zu haben scheinen, wenden Sie sich an das Cisco TAC mit den erforderlichen Details über die Version des Anrufmanagers, die Anzahl der Knoten im Cluster, die Zeit und die Dauer der Warnung sowie die erforderliche Prozessverengung bei CPU-Pegging.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.