

Alertes de l'outil de surveillance en temps réel

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Alertes RTMT](#)

[Configuration](#)

[Alertes système](#)

[Alertes CallManager](#)

[LowAvailableVirtualMemory et LowSwapPartitionAvailableDiskSpace](#)

[LogPartitionHighWaterMarkExceeded et LogPartitionLowWaterMarkExceeded](#)

[PeggingUC](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document discute des alertes RTMT (Real-Time Monitoring Tool) de Cisco et explique comment dépanner certaines alertes courantes.

Conditions préalables

Conditions requises

Cisco recommande que vous connaissiez l'administration Web de Cisco Call Manager.

Components Used

Les informations de ce document sont basées sur le serveur Cisco CallManager 11.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Informations générales

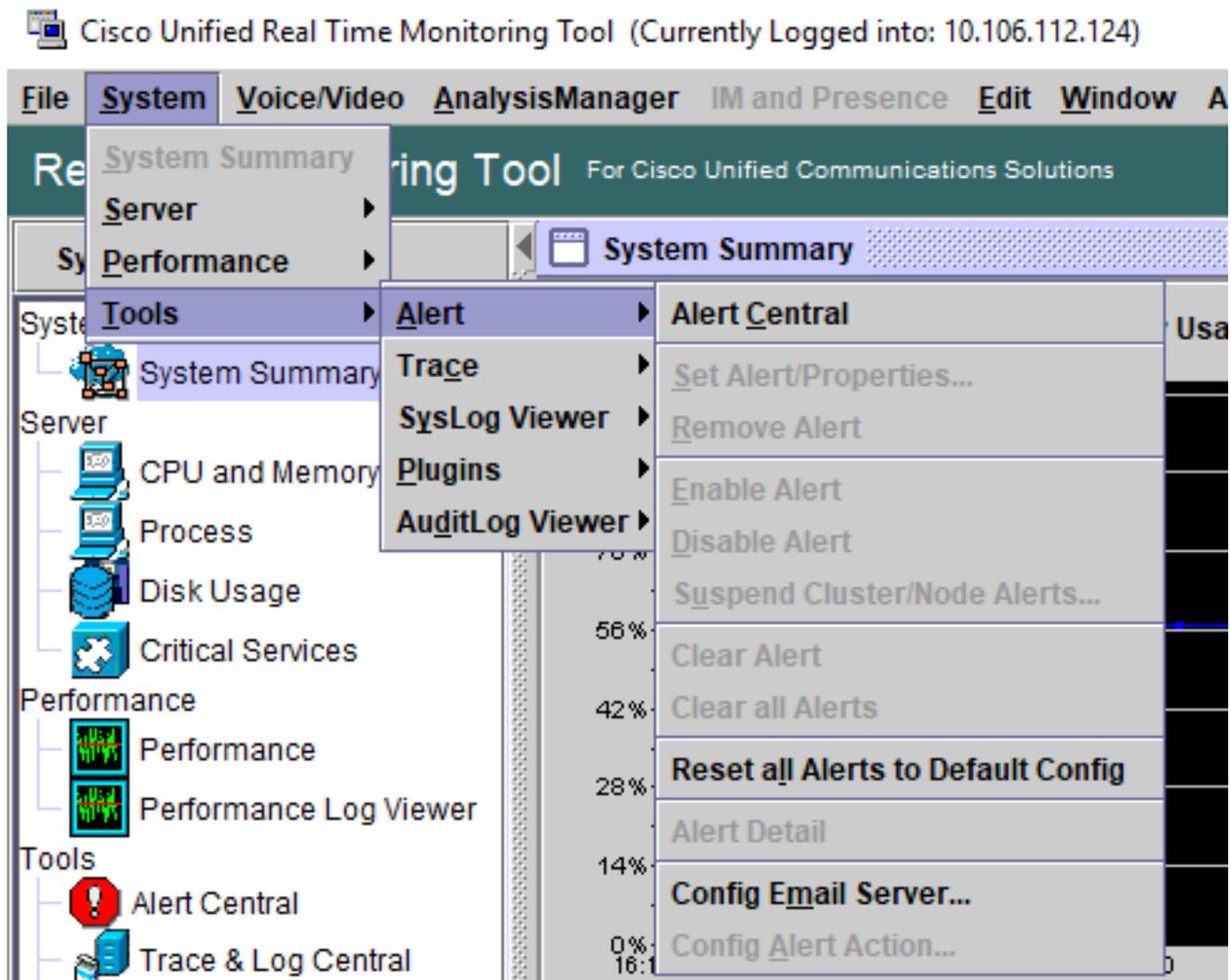
Le RTMT qui s'exécute en tant qu'application côté client utilise HTTPS et TCP afin de surveiller les performances système, l'état des périphériques, la détection des périphériques, les applications CTI (Computer Telephony Integration) et les ports de messagerie vocale. RTMT peut être utilisé pour configurer des alertes pour le cluster qu'il surveille.

Le système génère des messages d'alerte afin d'avertir l'administrateur lorsqu'une condition prédéfinie est remplie, par exemple lorsqu'un service activé passe de up to down. Le système peut envoyer des alertes par e-mail/page électronique.

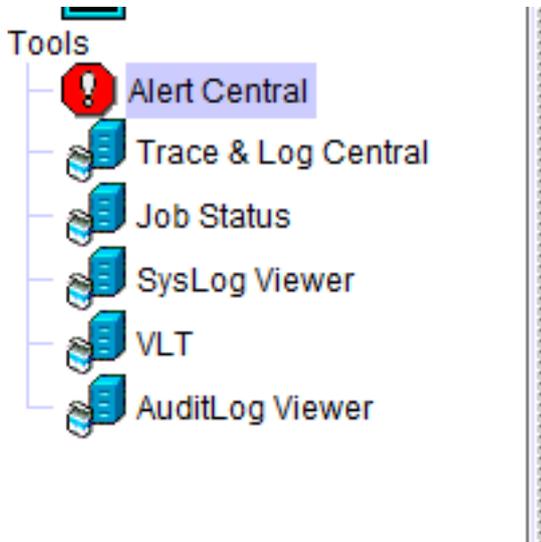
RTMT, qui prend en charge la définition, la définition et l'affichage des alertes, contient des alertes préconfigurées et définies par l'utilisateur. Bien que vous puissiez effectuer des tâches de configuration pour les deux types, vous ne pouvez pas supprimer les alertes préconfigurées.

Alertes RTMT

Unified RTMT affiche à la fois des alertes préconfigurées et des alertes personnalisées dans Alert Central, comme le montre l'image.



Vous pouvez également accéder à Alert Central en cliquant sur l'icône Alert Central dans l'arborescence hiérarchique du tiroir système.



Configuration

Unified RTMT organise les alertes sous les onglets applicables : Système, CallManager, Cisco Unity Connection et Personnalisé.

Alert Central		
System	Voice/Video	Custom
Alert Name		Enabled
ILSPwdAuthenticationFailed		Enabled
ILSTLSAuthenticationFailed		Enabled
IMEDistributedCacheInactive		Enabled
IMEOverQuota		Enabled
IMEQualityAlert		Enabled
IMEServiceStatus		Enabled
InsufficientFallbackIdentifiers		Enabled
InvalidCredentials		Enabled
LocationOutOfResource		Enabled
MaliciousCallTrace		Enabled

Vous pouvez activer ou désactiver des alertes préconfigurées et personnalisées dans Alert Central ; toutefois, vous ne pouvez pas supprimer les alertes préconfigurées.

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

Les alertes dans RTMT sont classées comme suit :

- [Alertes système](#)
- [Alertes CallManager](#)
- Alertes personnalisées

Alertes système

Cette liste comprend les alertes système préconfigurées :

- Échec de l'authentification
- CiscoDRFFailure
- FichierDumpBaseTrouvé
- PeggingUC
- CriticalAuditEventGenerated
- CriticalServiceDown
- Défaillance matérielle
- ChaîneRechercheFichierJournalTrouvé
- LogPartitionHighWaterMarkExceeded
- LogPartitionLowWaterMarkExceeded
- EspaceDisqueDisponibleFaiblePartitionActive
- MémoireVirtuelleFaibleDisponible
- FaiblePartitionInactiveEspaceDisqueDisponible
- EspaceDisqueDisponiblePartitionFaibleÉchange
- ServerDown (s'applique aux clusters Unified Communications Manager (CUCM))

- SparePartitionHighWaterMarkExceeded
- SparePartitionLowWaterMarkExceeded
- SyslogSeverityMatchFound
- SyslogStringMatchFound
- VersionSystèmeNon concordante
- TotalProcessesEtThreadsDépasséSeuil

Alertes CallManager

Cette liste comprend les alertes CallManager préconfigurées.

- BeginThrottlingCallListBLFSubscriptions
- CallAttemptBlockedByPolicy
- CallProcessingNodeCpuPegging
- CARIDSEngineCritical
- CARIDSEngineFailure
- ÉchecTâchePlanificateurCARS
- Échec de CDRAgentSendFileFailed
- ÉchecLivraisonFichierCDRF
- DépassementMarkEauSupérieurCDRHigh
- CDRMaximumDiskSpaceDépassé
- CodeJaune
- DBChangeNotifyFailure
- DBReplicationFailure
- DBReplicationTableOutOfSync
- DDRBlockPrevention
- DDRDown
- EMCCFailInLocalCluster
- EMCCFailInRemoteCluster
- RapportsQualitéVocale excessifs
- IMEDistributedCacheInactive
- IMEOverQuota
- AlerteQualitéIMEQ
- IdentificateursFallback insuffisants
- IMEServiceStatus
- Informations d'identification non valides
- FaibleFréquenceFréquenceDeCoeurTFTPServer
- SuiviAppelMalveillant
- MediaListExhausted
- MgcPDChannelOutOfService
- NombreDePériphériquesEnregistrésDépassé
- NombreDePasserellesEnregistréesDiminué
- NombreDePasserellesEnregistréesAugmenté
- NombreDePériphériquesSupportEnregistrésDiminué
- NombreDePériphériquesSupportEnregistrésAugmenté

- NombreDeTéléphonesEnregistrésAbandonnés
- RouteListExhausted
- SDLLinkOutOfService
- TCPSetupToIMEFail
- TLSConnectionToIMEFail
- ÉchecEntréeUtilisateur

LowAvailableVirtualMemory et LowSwapPartitionAvailableDiskSpace

Les serveurs Linux ont tendance à 'ne pas effacer' l'utilisation de la mémoire virtuelle sur une période de temps et on a vu qu'elle s'accumulait et donc ces alertes.

```

|LowActivePartitionAvailableDiskSpace
|LowAvailableVirtualMemory
|LowInactivePartitionAvailableDiskSpace
|LowSwapPartitionAvailableDiskSpace
|ServerDown

```

Linux fonctionne un peu différemment en tant que système d'exploitation.

Une fois la mémoire allouée à un processus, elle ne sera pas récupérée par le processeur à moins que d'autres processus ne demandent plus de mémoire que la mémoire disponible.

Cela entraîne une mémoire virtuelle élevée.

Une demande d'augmentation du seuil de l'alarme dans les versions supérieures du gestionnaire d'appels a été documentée dans le défaut ;

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

Pour les partitions d'échange, cette alerte indique que la partition d'échange est laissée avec peu d'espace disponible et est fortement utilisée par le système. La partition d'échange est normalement utilisée pour étendre la capacité de mémoire vive physique lorsque nécessaire. Dans des conditions normales, si la mémoire vive est suffisante, le swap ne doit pas être trop utilisé.

En outre, il peut s'agir d'alertes RTMT déclenchées par une accumulation de fichiers temporaires, un redémarrage du serveur est recommandé pour effacer les fichiers temporaires inutiles.

LogPartitionHighWaterMarkExceeded et LogPartitionLowWaterMarkExceeded

Lors de l'exécution de **show status** sur l'interface de ligne de commande d'un serveur CUCM, une valeur qui spécifie le pourcentage occupé et libre de la partition de journalisation dans l'espace disque CUCM est affichée. Également appelées partitions courantes, ces valeurs spécifient l'espace occupé par les journaux/traces et les fichiers CDR dans le serveur, qui, même s'ils sont inoffensifs, peuvent causer des problèmes dans la procédure d'installation/mise à niveau en raison d'un manque d'espace au fil du temps. Ces alertes servent d'avertissement à l'administrateur pour effacer les journaux qui se sont accumulés au fil du temps dans le cluster/serveur.

LogPartitionLowWaterMarkExceeded : cette alerte est générée lorsque l'espace rempli atteint les valeurs de seuil configurées pour l'alerte. Cette alerte sert d'indicateur de pré-vérification de l'utilisation du disque.

LogPartitionHighWaterMarkExceeded : cette alerte est générée lorsque l'espace rempli atteint les valeurs de seuil configurées pour l'alerte. Une fois l'alerte générée, le serveur commence à purger automatiquement les journaux les plus anciens afin de réduire l'espace à la valeur des pertes que le seuil HighWaterMark.

Il est recommandé de purger les journaux manuellement dès que l'alerte LogPartitionLowWaterMarkExceeded est reçue.

Pour ce faire, il convient de :

Étape 1. Lancer RTMT.

Étape 2. Sélectionnez **Alert Central**, puis effectuez les tâches suivantes :

Sélectionnez **LogPartitionHighWaterMarkExceeded**, notez sa valeur et modifiez sa valeur de seuil à 60 %.

Sélectionnez **LogPartitionLowWaterMarkExceeded**, notez sa valeur et modifiez sa valeur de seuil à 50 %.

L'interrogation a lieu toutes les 5 minutes, donc attendez 5 à 10 minutes, puis vérifiez que l'espace disque requis est disponible. Si vous souhaitez libérer plus d'espace disque dans la partition commune, modifiez à nouveau les valeurs de thread LogPartitionHighWaterMarkExceeded et LogPartitionLowWaterMarkExceeded en valeurs inférieures (par exemple, 30 % et 20 %).

Donnez-lui 15 à 20 minutes pour libérer l'espace dans la partition commune. Vous pouvez surveiller la diminution de l'utilisation du disque à l'aide de la commande **show status** à partir de l'interface de ligne de commande.

Cela ferait tomber la partition commune.

PeggingUC

L'alerte CpuPegging surveille l'utilisation du CPU sur la base du seuil configuré.

Lorsque l'alerte d'identification de l'origine des besoins du processeur est reçue, le processus qui occupe le processeur le plus élevé peut être occupé en accédant au tiroir système à gauche, c'est-à-dire Processus.

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

À partir de l'interface de ligne de commande du serveur concerné, ces résultats donneront un aperçu.

- test de diagnostic utils
- show process load cpu trié
- show status
- liste active principale utils

Il est recommandé d'observer si la pointe du CPU se produit à un moment spécifique ou de manière aléatoire. S'il se produit de façon aléatoire, alors les traces détaillées de CUCM requises ainsi que les journaux de perfmon RisDC pour vérifier ce qui déclenche le pic dans le CPU. Si les alertes se produisent à une heure spécifique de la journée, cela peut être dû à une activité planifiée comme la sauvegarde du système de reprise après sinistre (DRS), la charge CDR, etc.

En outre, sur la base des informations sur le processus qui occupe le plus de CPU, des journaux spécifiques sont pris pour une enquête plus approfondie. Par exemple. si le coupable est Tomcat, les journaux associés à Tomcat sont nécessaires.

```
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
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Si les alertes ne sont pas rejetées après que vous ayez suivi les solutions proposées ici, ou si elles semblent avoir un impact immédiat sur le service, contactez le centre d'assistance technique de Cisco pour obtenir les détails nécessaires sur la version du gestionnaire d'appels, le nombre de nœuds dans le cluster, l'heure et la durée de l'alerte et le processus requis en cas d'identification par le processeur.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.