

Identificeer onverwachte sluiting in UCS-toepassing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Controleer of de installatie niet correct is uitgeschakeld](#)

Inleiding

Dit document beschrijft hoe u een onverwachte afsluiten van een toepassing bovenop het aangepaste Cisco Voice Operating System (VOS) kunt identificeren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie


De Cisco Unified Communications Manager (CUCM), Cisco Unity Connection (CUC), Cisco Unified Contact Center Express (UCX), Cisco Emergency Responder (CER) en Cisco Prime worden beschouwd als UC-toepassingen.

Als de server onverwacht wordt afgesloten, kan de consistentie van het bestandssysteem niet worden gegarandeerd. Bestanden kunnen onverwachts worden verwijderd, de eigendom van bestandstoestemmingen kan worden gewijzigd of de inhoud van bestanden kan worden beschadigd.

Om het systeem tijdelijk te kunnen herstellen, voert u de system recovery disk uit die is vrijgegeven voor de corresponderende softwareversie.

Controleer of de installatie niet correct is uitgeschakeld

Bekijk de system-history.log om te bepalen of een systeem niet correct is afgesloten.

 **Opmerking:** het bestand history.log is uitgebreid om onjuiste sluitingen met Cisco bug-id [CSCtr8859](#) te kunnen volgen om alarmen en waarschuwingen toe te voegen voor onverwachte herstart die in CUCM-versies 9.1(1) en hoger zijn geïntegreerd.

1. Download de installatie-/upgrade-logbestanden van de Cisco Unified Real-Time Monitoring Tool (RTMT) en verzamel de systeemgeschiedenis.log.

of

Voer de opdracht system-history.log in in de bestandsweergave op de opdrachtregelinterface (CLI).

2. Bekijk elke instantie van root: Boot en bevestig dat elke instantie wordt voorafgegaan door een van deze regels:

```
root: Restart  
root: Shutdown  
root: Install  
root: Upgrade
```


3. Als een opstartexemplaar niet wordt opgestart door een herstart, afsluiten, installeren of upgraden, was er waarschijnlijk een onschone sluiting.

Dit is een voorbeeld van een onschone shutdown:

```
08/14/2012 13:36:09 | root: Boot 9.0.1.10000-37 Start  
08/14/2012 17:28:25 | root: Boot 9.0.1.10000-37 Start
```

In dit voorbeeld moet de server opnieuw worden opgebouwd om de consistentie van het bestandssysteem te garanderen. Zie deze Cisco bug-id's voor meer informatie:

- Cisco bug-id [CSCth60800](#), "Herstel Schijf waarschuwing om systeem na reparatie bestandssysteem te herbouwen"
- Cisco bug-id [CSC53322](#), "Documenteer de noodzaak van systeemherbouw na reparatie bestandssysteem"
- Cisco bug-id [CSCuy94644](#), "Cisco Emergency Responder-corruptie na onverwachte sluiting"

 Opmerking: als de server op VMware draait op een versie zonder de fix voor Cisco bug ID [CSCtw73590](#), "VSphere geïnitieerde afsluiten of opnieuw opstarten niet gelogd op system-history.log" en als de server is uitgeschakeld door VSphere wanneer een gastsluiting wordt geïnitieerd, is die vermelding niet opgenomen in de system-history.log.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.