ACS 5.x: Esempio di sincronizzazione di Cisco ACS con il server NTP

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[Configurazione](#)
[Configurazione NTP su Cisco ACS](#)
[Verifica](#)
[Risoluzione dei problemi](#)
[Problema: Il clock si allontana eccessivamente e l'NTP si interrompe quando ACS è installato su un computer VMWare](#)
[Soluzione](#)
[Sincronizzazione NTP persa dopo la modifica dell'indirizzo IP dell'interfaccia ACS](#)
[Soluzione](#)
[Informazioni correlate](#)

Introduzione

Il protocollo NTP (Network Time Protocol) è un protocollo utilizzato per sincronizzare gli orologi di diverse entità di rete. Utilizza UDP/123. L'obiettivo principale di questo protocollo è evitare gli effetti della latenza variabile sulle reti di dati.

In questo documento viene fornito un esempio di configurazione in cui Cisco ACS sincronizza l'orologio con il server NTP. ACS 5.x può configurare fino a due server NTP.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure ACS versione 5.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Configurazione NTP su Cisco ACS

Per sincronizzare l'ora del Cisco ACS con un server NTP, attenersi alla seguente procedura:

1. Configurare manualmente la data e l'ora con il comando **clock set <month> <day> <hh:min:ss> <yyyy>**.
2. Specificare il fuso orario con il comando **clock timezone<timezone>** .
3. Specificare il server NTP con il comando **NTP server <indirizzo IP del server NTP>**.Il protocollo NTP segue una gerarchia client-server. Quando un client NTP è configurato con un server NTP, l'*orologio* di *riferimento* del server NTP viene passato al client. Sono necessari circa 10-20 minuti per ottenere l'ora esatta dal server NTP e dipende dal verificarsi del ritardo per raggiungere il server NTP.Cisco ACS utilizza il daemon NTP per sincronizzare l'orologio con il server NTP. Non supporta il protocollo SNTP, SNTP. Quando il daemon NTP si avvia, ACS invia un pacchetto al server NTP contenente l'ora originale (locale). Quindi il server NTP risponde al pacchetto con l'inserimento della sua ora di clock di riferimento. Quando il client NTP riceve questo pacchetto, lo registra con la propria ora locale per convalidare il tempo di viaggio impiegato dal pacchetto. Si verificano diversi scambi di pacchetti di questo tipo per calcolare il tempo di ritardo di andata e ritorno esatto e i valori di offset e infine l'ora locale del client NTP è sincronizzata con l'orologio di riferimento del server NTP.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Per verificare i dettagli della configurazione, fare riferimento a questi frammenti di output del comando.

```
acs51/admin#show clock
```

```
Wed Jun 13 11:02:00 IST 2012
acs51/admin#

acs51/admin(config)#ntp server 192.168.26.55
The NTP server was modified.
If this action resulted in a clock modification, you must restart ACS.
acs51/admin(config)#

acs51/admin#show ntp
Primary NTP   : 192.168.26.55

synchronised to NTP server (192.168.26.55) at stratum 2
   time correct to within 27 ms
   polling server every 64 s

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
127.127.1.0     LOCAL(0)        10 l   29   64   17    0.000    0.000   0.001
*192.168.26.55   .LOCL.           1 u   33   64   17    0.285   -9.900   2.733

Warning: Output results may conflict during periods of changing synchronization.
```

Nota: *Stratum* è una misura che specifica quanto il server NTP è vicino all'orologio di riferimento primario. Ogni client NTP sincronizzato con uno strato *n* server viene definito a livello di strato n+1.

Per verificare i dettagli della sincronizzazione NTP, fare riferimento a questi messaggi di log delle applicazioni inviati da ACS.

```
acs51/admin# show logging application | in ntp
Jun 13 13:51:59 acs51 ntpd[20259]: ntpd 4.2.0a@1.1190-r Mon Jul 28 11:03:50 EDT 2008 (1)
Jun 13 13:51:59 acs51 ntpd[20259]: precision = 1.000 usec
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface wildcard, 0.0.0.0#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface wildcard, ::#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface lo, 127.0.0.1#123
Jun 13 13:51:59 acs51 ntpd[20259]: Listening on interface eth0, 192.168.26.51#123
Jun 13 13:51:59 acs51 ntpd[20259]: kernel time sync status 0040
Jun 13 13:51:59 acs51 ntpd[20259]: frequency initialized 0.000 PPM from /var/lib/ntp/drift
Jun 13 13:51:59 acs51 ntpd: ntpd startup succeeded
Jun 13 13:55:15 acs51 ntpd[20259]: synchronized to 192.168.26.55, stratum 2

!--- Output suppressed-
```

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Problema: Il clock si allontana eccessivamente e l'NTP si interrompe quando ACS è installato su un computer VMWare

Cisco ACS è configurato per utilizzare il server NTP come origine dell'orologio, ma viene continuamente modificato nell'origine dell'ora interna. In questo caso, non consente agli utenti di eseguire l'autenticazione da Active Directory, in quanto Kerberos supporta solo 300 secondi di

differenza di tempo.

Soluzione

Quando l'host ESXi utilizza la CPU in modo elevato, non serve le VM con la stessa frequenza del normale. Ciò influisce sugli orologi all'interno delle VM e provoca in effetti una deviazione dell'orologio da un controller di dominio Windows superiore a cinque minuti. Provoca il fallimento di Kerberos. Questo avrebbe un impatto anche su una VM Windows senza NTP o sincronizzazione dell'orologio host. Poiché l'orologio virtuale presentato ad ACS Cisco non è sufficientemente stabile da consentire al NTP di stare al passo con la deriva, alla fine torna a utilizzarsi come sorgente di tempo.

Nota: il daemon NTP regola l'orologio in diversi scambi e continua finché il client non ottiene l'ora esatta. Tuttavia, quando il ritardo tra il server NTP e il client NTP diventa troppo grande, il daemon NTP viene terminato ed è necessario regolare manualmente l'ora e riavviare il daemon NTP.

Questo problema è destinato a essere risolto quando si integra il supporto degli strumenti VMWare in Cisco ACS, disponibile con Cisco ACS release 5.4 non ancora pubblicata. per ulteriori informazioni, fare riferimento all'ID bug Cisco CSCtg50048 (solo utenti registrati). Come soluzione temporanea, è possibile provare la seguente procedura:

- Arrestare i servizi ACS con il comando **ACS stop**.
- Rimuovere tutta la configurazione NTP e salvarla con un comando **write mem**.
- Riavviare Cisco ACS.
- Verificare che tutti i servizi siano in esecuzione con il comando **show application status acs**.
- Impostare l'orologio in modo che sia il più vicino possibile al tempo reale, al secondo prima del requisito di offset su NTP.
- Assicurarsi che il fuso orario sia corretto.
- Aggiungere nuovamente la configurazione NTP e salvarla.
- Eseguire il comando **show ntp** per verificare se l'output è lo stesso.

Nota: se questa procedura non risolve il problema, si consiglia di contattare Cisco TAC.

Sincronizzazione NTP persa dopo la modifica dell'indirizzo IP dell'interfaccia ACS

Se si modifica l'indirizzo IP della scheda NIC ACS, il protocollo NTP non sarà più sincronizzato.

Soluzione

Questo comportamento viene osservato e registrato nel bug Cisco con ID CSCtk76151 (solo utenti registrati). Quando l'indirizzo IP ACS viene modificato, l'applicazione ACS viene riavviata ma non il daemon NTP. Questa condizione è stata risolta in ACS versione 5.3.0.23. Per risolvere il problema nelle versioni precedenti, attenersi alla seguente procedura:

1. Usare il comando **no ntp server** per interrompere il processo NTP.
2. Rieseguire il comando **ntp server** per riavviare il processo NTP.

Informazioni correlate

- CS ACS 5.X - Supporto prodotti

- Guida per l'utente di Cisco Secure Access Control System 5.3
- Documentazione e supporto tecnico – Cisco Systems