Corso di SGR 2000/2001

Realizzazione di un MIB SNMP per il controllo del servizio syslog

Di
Bruni Eden
Diploma di Informatica
Università degli studi di Pisa
Pisa
Italy
E-Mail: bruni@cli.di.unipi.it

1. Introduzione

Con la crescita di Internet, si sono diffuse più velocemente le reti locali basate sulla famiglia di protocollo TCP/IP. I nuovi servizi telematici hanno avvicinato nuove fasce di utenti all'uso del

computer connesso in rete, contribuendo all'aumento delle infrastrutture. Di conseguenza ci sono voluti dispositivi sempre più evoluti e complessi, e si sono presentate situazioni più complicate da gestire. Il problema che si presenta è l'affidabilità e la sicurezza nei confronti della rete, quindi i tecnici responsabili si sono trovati a controllare assiduamente per poter risolvere tempestivamente ogni possibile problema.
Per risolvere il problema nella famiglia TCP/IP, il modello che ha riscontrato maggior successo è SNMP (Simple Network Management Protocol, protocollo per la gestione di rete TCP/IP). Questo protocollo fin dalla prima volta (1988) si è presentato come un valido strumento per amministrare le reti IP.
Per il modello Network Management si prevede l'uso di due unita': manager e agent. Il protocollo SNMP, decide le regole e la forma dei messaggi che le due si devono scambiare per le informazioni.
Il modello manager-agent non è altro che una variante del client-server.
Il ruolo del client è svolto dal manager che si occupa di interrogare gli agent e raccogliere in un database le informazioni. Mentre il funzionamento dell'agent è come quello del server, rispondono a comandi inviati da uno o più manager. Comunque se occorre un agent può produrre informazioni non richieste per informare il manager di un evento particolare.
La versione più recente di SNMP prevede la formazione di strutture gerarchiche tra menager per far sì che i manager comunichino tra di loro.
Oltre al protocollo SNMP, il sistema Network Management per reti TCP/IP ha altre due componenti:
- un sistema di risorse amministrabile con SNMP, organizzato in un'unica struttura standard, un'unica base dati denominata MIB (Management Information Base);
- una modalità standard per riferire gli elementi che costituiscono la MIB.
La MIB è una base che specifica tutte le risorse gestibile da remoto dall'amministratore di rete. Questa base definisce per ogni elemento che fa parte dell'infrastruttura di rete, una serie di oggetti accessibili via SNMP.
Il protocollo SNMP è del tipo richiesta/risposta, il manager ha a disposizione vari messaggi con cui interrogare l'agent. Ci sono varie versioni di SNMP, la più recente è SNMPv3 la cui prevede i seguenti messaggi, da manager a agent:
- Get-Request per sollecitare l'invio d'informazioni relativa ad una o più variabili MIB;
- Get-Next Request per sollecitare l'invio d'informazioni successive, correlata con le informazioni appena ricevute;
- Get Bulk-Request per sollecitare l'invio di un insieme d'informazioni, senza necessità di ulteriori richieste;
- Set-Request per modificare il valore di una o più variabili BIM.

Questi messaggi sono inviati utilizzando il protocollo UDP (Porta 162).
I messaggi previsti da agent a manager sono invece:
- Get-Responser che contiene le informazioni richieste da un precedente Request;
- Trap per la notificazione al manager di particolari eventi avvenuti sulla stazione che ospita l'agent.

Le Trap utilizzano la Porta 161, sostanzialmente servono per comunicare fra l'agent e la console di gestione. Quindi è l'agent ad inviare un messaggio verso il manager in seguito al fallimento di un controllo configurato. Sostanzialmente serve per registrare eventi particolari verificatosi su un dispositivo di interconnessione.

2. Il MIB

Il MIB SNMP in questione si occupa di tener traccia dei messaggi riportati nel syslog in un'applicazione di sistema Unix, in particolar modo definisce Trap per allertare gli amministratori di sistema quando si verificano allarmi di particolare gravita'.

Il problema è stato risolto specificando una tabella nel MIB dove sono presenti colonne, ognuna denominata con un nome specifico, che servono per monitorare l'andamento dei messaggi. Le voci utilizzate sono le seguenti: uNomeProcesso, ULivello, UContatore, uInviaTrap.
La tabella ha quattro colonne che servono a catalogare i messaggi ogni volta che arrivano, più dettagliatamente.
UNomeProcesso si occupa di associare un nome a ogni file di syslog che si presenta di modo da identificarlo in tabella.
ULivello si occupa di definire il livello di syslog sotto il quale viene emessa una Trap. I livelli più allarmanti sono compresi da 0 a 3.
UContatore si occupa di contare i numero di messaggi emessi, viene incrementato ogni volta che viene emessa una Trap.
UInviaTrap si occupa di definire quando allertare gli amministratori con una Trap; emette 1 che è = invia Trap altrimenti emette 0 che è = non inviare Trap.

Trap-MIB **Definitions** ::= **BEGIN**

IMPORTS……..

TrapMIB **MODULE-INDENTITY**
LAST-UPDATED “0109191311Z”
ORGANIZATION “Università di Pisa”
CONTACT-INFO “Eden Bruni
Diploma di Informatica
Università degli studi di Pisa
Pisa, Italy
bruni@cli.di.unipi.it”
DECRIPTION
Questo MIB SNMP tiene traccia dei messaggi riportati nel syslog e secondo la gravità identificata dal livello, emette una Trap per allertare gli amministratori.”
::={private 64}

userTable **OBJECT-TYPE**
SYNTAX SEQUENCE OF userEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
“Tabella contenente i dati relativi ai messaggi di syslog per allertare gli amministratori, un’ipotesi buona è monitorare l’andamento con una tabella”
::={TrapMIB 1}

userEntry **OBJECT-TYPE**
SYNTAX userEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPITION
"Entry relative agli utenti"
::={ UserTable 1 }

userEntry ::= **SEQUENCE{**
uNameProcesso **OCTECT STRING**
uLlivello **UNSIGNED32**
uContatore **UNSIGNED32**
uInviaTrap **UNSIGNED32**
}

uNomeProcessso **OBJECT-TYPE**
SYNTAX OCTECTSTRING
MAX-ACCESS read-write
STATUS current
DESCRIPTION
"User name associato ad ogni file syslog che appare e quindi presente in tabella"
::={ userEntry 1 }

uLivello **OBJECT-TYPE**
SYNTAX UNSIGNED32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Livello per definire se emettere la Trap, se il livello va da 0 a 3 compreso emette Trap e incrementa il contatore, e quindi presenta in tabella”

::={userEntry 2}

uContatore **OBJECT-TYPE**
SYNTAX UNSIGNED32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Contatore che viene incrementato ogni volta che viene emessa una Trap, e quindi presente in tabella"
::={ userEntry 1 }

uInviaTrap **OBJECT-TYPE**
SYNTAX UNSIGNED32(0,1)
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"1 = inviare Trap , il livello è compreso tra 0 e 3 compresi; 0 = non inviare Trap, il livello è compreso tra 4 e 7 compresi e quindi presente in tabella"
::={ userEntry 1 }

3. CONCLUSIONI

Con questo MIB si è cercato un modo semplice per poter monitorare i messaggi d'errori riportati nel syslog, utilizzando una tabella dove vengono analizzati i messaggi nei loro particolari.
Il progetto è stato svolto nel seguente modo per questioni di tempo, ma può essere modificato in futuro ampliandolo più specificatamente.
Al progetto si possono apportare diverse modifiche, tutte mirate a migliorare l'utilizzo del MIB, perché più è dettagliato, più da informazioni.
Nel progetto può essere rivista la formulazione della tabella specificandola più nel dettaglio.

Le variazioni nel MIB potrebbero essere del tipo: di aggiungere più voci nella tabella, ad esempio di specificare più precisamente la provenienza degli errori riportati dei syslog di modo che possa valutare meglio il messaggio, e capirne la gravità dell'errore per aiutare alla risoluzione del problema, perché più i dettagli vengono fatti chiari agli amministratori più questi sono in grado di intervenire tempestivamente sul problema.
Si possono aggiungere tante altre voci interessanti ad esempio una voce che mi aiuta a monitorare l'ora e la data del messaggio, un'altra voce che mi dice da quale macchina il processo stava girando, etc.

4. RIFERIMENTI

- "Sistemi di Elaborazione dell'Informazione: Gestione di Rete"
  di J. Shoenwalder – L. Deri
- "Internet Security"
  Editore Ulrico Hoepli Milano
- "http:://digilander.iol.italberanid/doc/syslog/syslog.html"