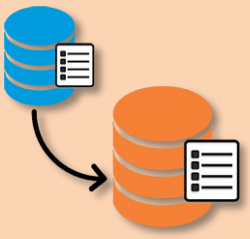
SECURSYS

milestone TECHNOLOGY PARTNER

milestone VERIFIED



LogSync

MIP Plugin per l'accodamento dei messaggi di Audit Log su Server SysLog

Rev. 2.0.0.0

Guida dell'Utente

Tabella delle Revisioni

Rev.	Data	Modifiche
1.0.0.0	09/12/2019	Prima Emissione pubblica del Plugin
2.0.0.0	11/06/2020	Trasformazione dell'applicativo di accodamento su Server SysLog in Servizio di Windows

Sommario

1 Copyright e Limitazioni di Responsabilità

Limitazioni di Responsabilità

Questo documento è destinato esclusivamente a scopi di informazioni generali dell'Applicazione in oggetto e la sua applicazione alla Piattaforma Milestone XProtect, della quale è richiesta almeno una conoscenza di base.

Qualsiasi rischio derivante dall'uso di queste informazioni e/o dell'Applicazione stessa è di competenza del destinatario che non potrà in alcun caso rivalersi sul Produttore.

Tutti i riferimenti a impianti, persone e organizzazioni utilizzati nel documento sono fittizi e qualsiasi somiglianza con situazioni reali è puramente casuale e non intenzionale.

SecurSys si riserva il diritto di apportare modifiche all'Applicazione senza alcun preavviso.

2 Introduzione

Questa Applicazione è stata sviluppata allo scopo di inviare periodicamente tutti i messaggi accodati nel Registro Attività Utente (Audit Log) verso un Server SysLog configurato. La trasformazione dei messaggi di log della Piattaforma XProtect e l'invio degli stessi è conforme allo standard vigente, descritto nel RFC 5424 del marzo 2009.

La lettura, trasformazione e invio dei messaggi verso il Server SysLog è effettuato da uno specifico Servizio di Windows, chiamato **MipLogSyncQueueService**. Questo si attiva periodicamente (la frequenza è configurabile), legge dal registro di log di XProtect i messaggi aggiunti dopo l'ultima schedulazione, li trasforma come richiesto dallo standard di riferimento e li invia al Server SysLog, registrando le informazioni sull'ultimo invio effettuato, in modo da riprendere, alla schedulazione successiva, dal messaggio successivo.

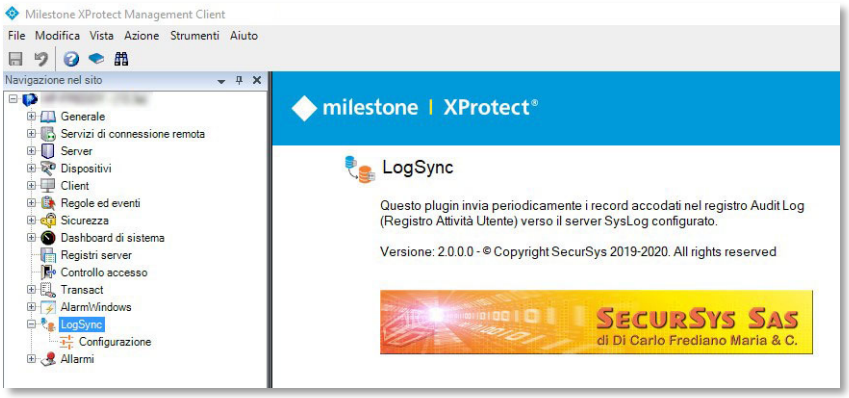
Per poter funzionare correttamente il Servizio ha bisogno di specifiche informazioni (credenziali per l'accesso alla piattaforma XProtect, parametri del Server SysLog, etc.) che gli Utenti devono configurare tramite il Plugin LogSync, che opera esclusivamente in ambiente Management Server.

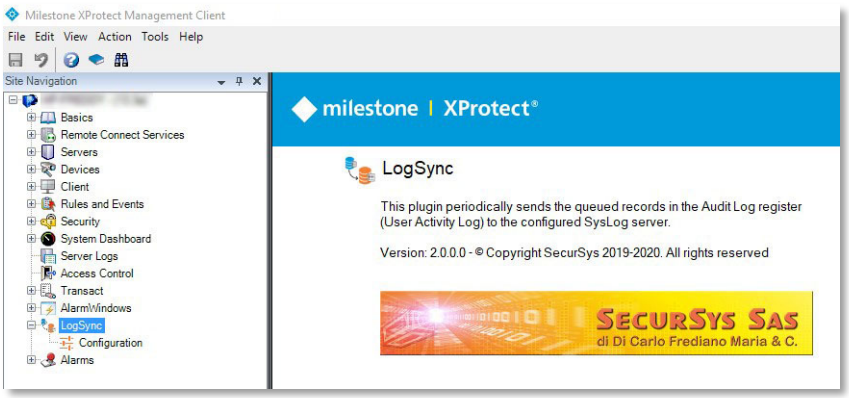
Il Plugin, visto che il Servizio non interagisce con l'Utente, può anche essere utilizzato per verificare il corretto funzionamento e lo stato di avanzamento dei trasferimenti.

2.1 Lingua Utilizzata dal Plugin

La versione attuale implementa la gestione delle lingue Italiana e Inglese, la cui scelta è automatica, legata alla lingua utilizzata dal Client.

La lingua Inglese rappresenta il default, pertanto su qualsiasi sistema dove non sia impostata la lingua Italiana il plugin si presenta in Inglese.





3 Procedura di Installazione

Il Plugin è dotato di due distinte procedure di installazione, una per il Plugin stesso e l'altra per il Servizio, che provvedono alla creazione delle cartelle contenenti quanto di necessario al corretto funzionamento.

La procedura di installazione del Plugin propone come cartella di destinazione **C:\Programmi\Milestone\MIPPlugins\LogSync**; il nome della cartella può anche essere modificato, ma non la posizione ..\MIPPlugins\ che è quella dove devono risiedere i Plugin su piattaforme a 64 bit; si consiglia comunque di lasciare inalterato l'intero percorso.

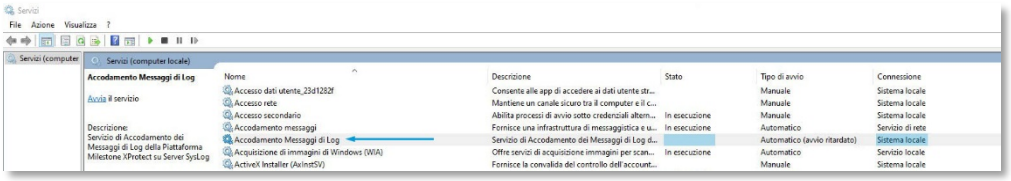
Si consiglia altresì di lasciare inalterati tutti i parametri della procedura di installazione del Servizio, per avere la certezza che venga correttamente installato e caricato in memoria all'avvio del Windows.

Nel caso di aggiornamento le procedure provvederanno prima dell'installazione alla disinstallazione della versione precedente.

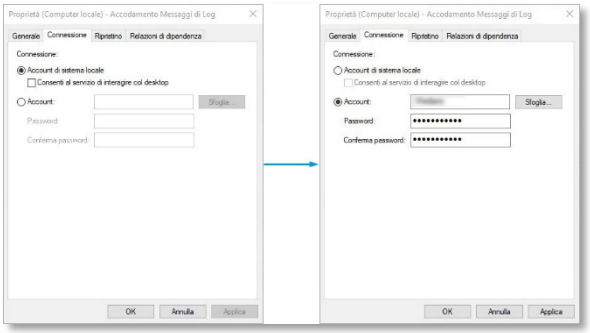
Non è necessario fermare alcun servizio di Milestone per effettuare l'installazione, il Plugin opera solo in ambito Management Client e fintanto che tale applicativo non è attivo il plugin non sarà residente in memoria.

ATTENZIONE – a causa dei continui aggiornamenti di Windows volti a incrementare la sicurezza del SO, dopo aver effettuato l'installazione del servizio, occorre fare in modo che sia avviato con privilegi di amministrazione, pena il corretto funzionamento dello stesso.
Seguire le seguenti istruzioni.

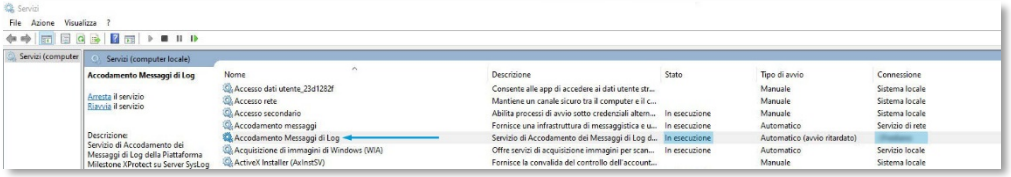
1. Aprire l'app Servizi di Windows
2. Fare doppio click sul Servizio



3. Selezionare il tab Connessione, quindi la voce Account e inserire le Credenziali e confermare



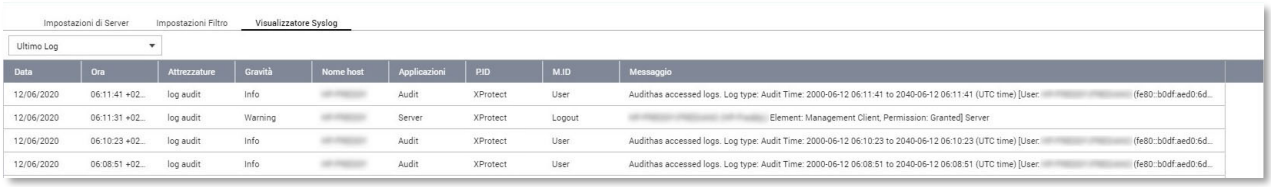
4. Avviare il Servizio



4 Specifiche sulla Trasformazione dei Dati di Log

Ciascun messaggio di log della Piattaforma XProtect ha un proprio formato, di seguito indicato come record, con propri campi, come illustrato nell'immagine seguente.

Analogamente esiste uno specifico tracciato record per SysLog, illustrato nell'immagine seguente.



Visto che parte dei campi di ciascun record differiscono tra loro si è reso necessario fare delle assunzioni (convenzioni) nella transcodifica dall'uno all'altro. In particolare:

- Milestone mostra la Data/Ora come Local Time, sebbene internamente utilizzi l'Universal Time, la Data/Ora inviata al SysLog è quella UTC che i client SysLog consentono di visualizzare in vari formati configurabili, quello dell'immagine è Universal Time più lo spostamento orario che tiene conto sia dal Fuso Orario, sia dell'Ora Solare/Legale (in pratica l'ora della prima riga è 08:11:41)
- Il campo SysLog indicato con Attrezzature, rappresenta per lo standard di riferimento il parametro Facility che può assumere valori da 0 a 23, ciascuno con il proprio significato; per questa applicazione è stato ritenuto più congruo il valore 13 che corrisponde al tipo "Log Audit"
- Il campo Gravità (del messaggio) è anch'esso codificato e può assumere 8 diversi valori (da 0 a 7), per la determinazione di tale campo sono state utilizzate le seguenti regole:
  - Se la Categoria del Log di XProtect è Sicurezza (Security) la Gravità assume il valore:
    - Alert, nel caso in cui l'operazione indicata non sia stata permessa
    - Warning, se l'operazione è stata eseguita
  - Per tutte le altre Categorie XProtect la Gravità assume il valore:
    - Warning, nel caso in cui l'operazione indicata non sia stata permessa
    - Info, se l'operazione è stata eseguita
- Il campo Nome Host viene valorizzato con il Nome della macchina che invia i record, ma NON può contenere l'eventuale nome di Domino
- Il campo Applicazioni corrisponde a quello "Tipo Sorgente" della piattaforma XProtect

- Il campo P.ID (Process ID) è sempre valorizzato con "XProtect"
- Il campo M.ID (Message ID) fornisce informazioni aggiuntive sul tipo di messaggio ed è normalmente utilizzato ai soli fini di ricerca; per esempio se i messaggi provenissero da uno switch o un firewall tale campo potrebbe assumere i valori "TCPIN" e "TCPOU" per differenziare il traffico in ingresso al dispositivo da quello in uscita. Quando non è esplicitamente valorizzato, come nel caso di questa applicazione, viene utilizzata la prima parola del contenuto informativo del messaggio
- Per finire il campo Messaggio è costruito a partire dal messaggio di log di XProtect (es. L'utente è acceduto con successo), al quale sono aggiunti gli altri campi di XProtect altrimenti non utilizzati, in pratica il Nome dell'Utente, la Fonte (Origine) e il Permesso (consesso/negato), in modo che tutte le informazioni rese disponibili da XProtect siano trasferite al Server SysLog.

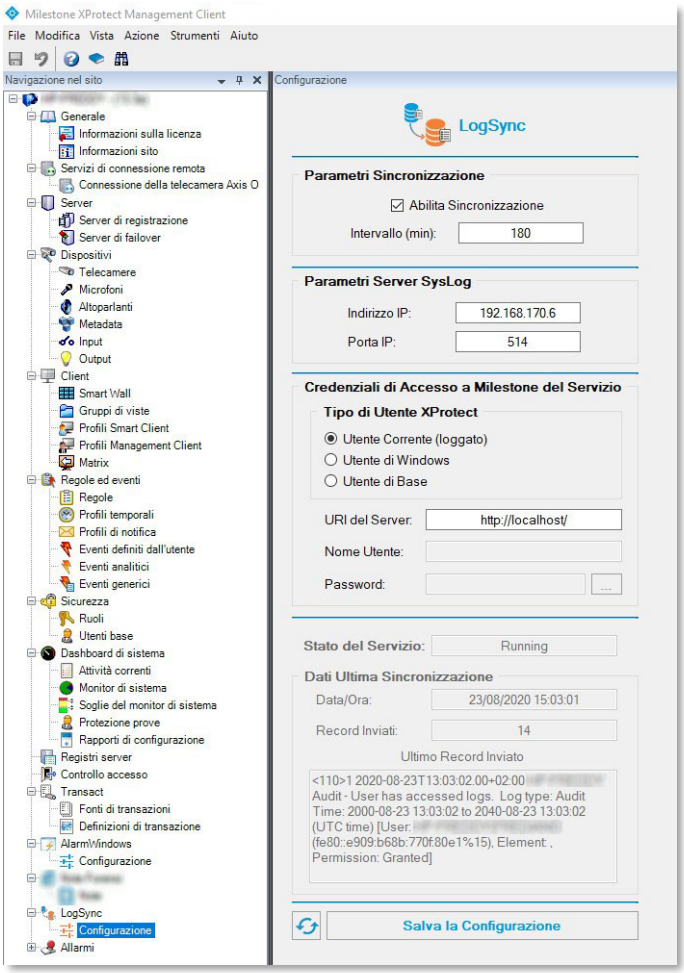
5 Operatività dell'Applicazione

Come indicato in precedenza, l'attività di trasferimento è interamente gestita dal Servizio di Windows, che però ha bisogno dei dati di configurazione impostati mediante il plugin.

5.1 Plugin

Il plugin opera esclusivamente in ambiente Management Client, pertanto per utilizzarlo è necessario avviare tale client; esso comparirà nell'albero degli oggetti gestiti da XProtect (sulla sinistra), come già illustrato nelle figure a pag. 5 relativo alle lingue disponibili.

Il Plugin dispone di una sola pagina per la configurazione dei Parametri di funzionamento e visualizzazione dello stato di avanzamento, come illustrato di seguito.



5.1.1 Parametri di Sincronizzazione

La sincronizzazione dei messaggi di Audit Log verso SysLog può essere sospesa e riabilitata tramite la spunta sulla relativa casella, è poi indispensabile specificare ogni quanti minuti deve essere attivata la procedura di sincronismo. Il valore minimo è 1', ma è decisamente consigliabile scegliere un intervallo dell'ordine di una o più ore, per i seguenti 2 motivi:

- Intervalli temporali piccoli tendono a trasferire un esiguo numero di messaggi e, visto che la procedura "ricorda" l'ultimo messaggio trasferito, non c'è alcuna possibilità qualcuno vada perduto[(1)]
- La schedulazione periodica induce un effetto collaterale dovuta al fatto che il Servizio, ad ogni schedulazione, accede (in lettura) al Registro di Log, cosa questa che viene a sua volta registrata dalla Piattaforma XProtect, quindi più sono ravvicinati i trasferimenti maggiore sarà la possibilità che sia trasferito il solo messaggio corrispondente all'accesso precedente del Servizio (e tanto maggiore sarà il numero di tali messaggi presenti su entrambe le piattaforme di log).

5.1.2 Parametri Server SysLog

Seguono i parametri per l'accesso al Server SysLog; per i motivi indicati nella nota non è possibile scegliere tra UDP e TCP, si usa sempre e solo il TCP, la porta è quella standard assegnata a tale servizio, ma può anche essere modificata.

5.1.3 Credenziali di Accesso a Milestone del Servizio

In questa sezione è necessario specificare le Credenziali di Accesso, e l'URI della Piattaforma, che deve utilizzare il Servizio di Windows per poter leggere i messaggi di log.

(1) L'affermazione non è del tutto corretta poiché il protocollo di trasporto non dispone di meccanismi di recupero contro l'eventuale perdita di pacchetti. Questo è tanto più vero se si utilizza il protocollo UDP, contemplato nello standard. Il servizio di Windows utilizza il protocollo TCP che garantisce maggiore affidabilità nel trasferimento.

Occorre specificare innanzi tutto che tipo di Utente deve accedere; le regole da rispettare sono le seguenti:

- Se il Tipo è Utente Corrente, cioè quello loggato su Windows, non c'è bisogno dei parametri di Account (Nome Utente e Password); la Piattaforma chiede all'Active Directory di Windows di chi si tratta, visto che tale servizio ha provveduto ad identificarlo; proprio per tale motivo la casella Nome Utente è valorizzata con l'account restituito da Windows
- Se il Tipo è Utente di Windows occorre indicare la Password (salvata cifrata e mai visibile) e l'account nella forma WinHost\Utente, dove WinHost rappresenta il nome dell'host di Windows cui compete l'autenticazione dell'Utente
- Se il Tipo è Utente di Base occorre indicare sia la password sia il Nome Utente che NON deve essere preceduto da alcun nome Host, visto che è la Piattaforma stessa ad autenticare questo tipo di Utente.

Per finire è presente l'Indirizzo (URI) del Server XProtect cui si desidera connettersi; se l'Applicazione gira sulla stessa macchina del server XProtect è sufficiente lasciare il parametro di default, in caso contrario occorre indicare l'Indirizzo IP o il Nome della Macchina, sempre preceduto dal suffisso http://.

Dopo aver effettuato le modifiche dei parametri si devono salvare le scelte fatte tramite l'apposito bottone in basso.

ATTENZIONE – in fase di salvataggio dei Parametri il Plugin comunica l'evento al Servizio di Windows che attiva una nuova schedulazione; questa prevede come prima operazione l'accesso ai parametri di Configurazione proprio per verificare che gli stessi non siano variati rispetto ai valori precedenti.
Nel caso il salvataggio avvenga proprio durante un ciclo di schedulazione sarà necessario attenderne il completamento prima di avviarne una nuova.

Nella parte bassa della pagina di configurazione sono riportati sia lo Stato del Servizio, sia i dati relativi all'ultima schedulazione dello stesso, in particolare:

- La Data/Ora dell'ultimo invio di messaggi al Server SysLog
- La quantità di messaggi inviati

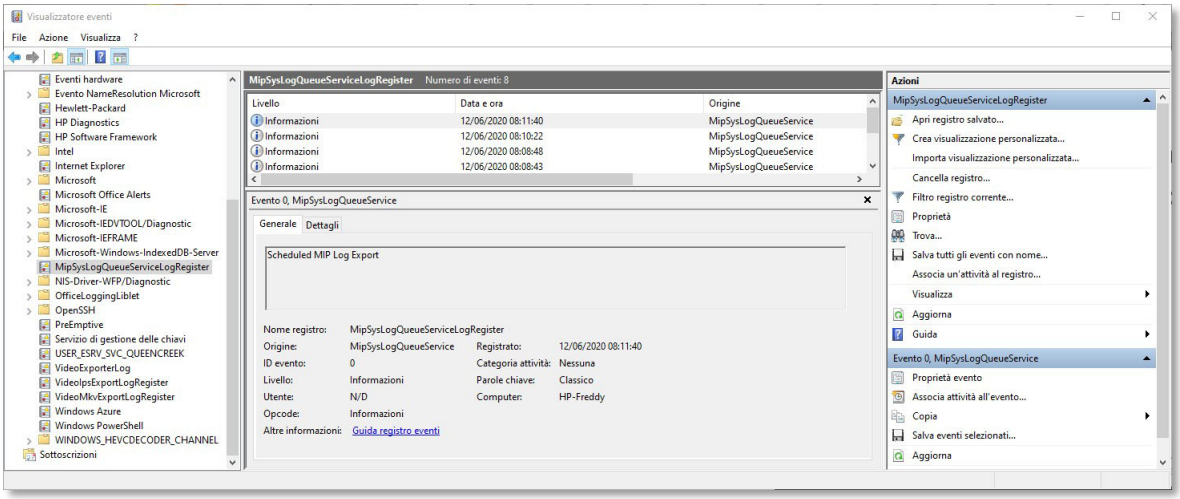
- Il contenuto informativo dell'ultimo messaggio TCP inviato

Si tratta di informazioni ai solo fini diagnostici, per essere certi che il Servizio stia facendo quando previsto. Il bottone in basso a sinistra con il simbolo di "Ricarica" permette di aggiornare tali informazioni.

Per il controllo delle attività del Servizio è anche possibile consultare, in alternativa, uno specifico registro di log di Windows dedicato all'applicazione, chiamato

MipSysLogQueueServiceLogRegister

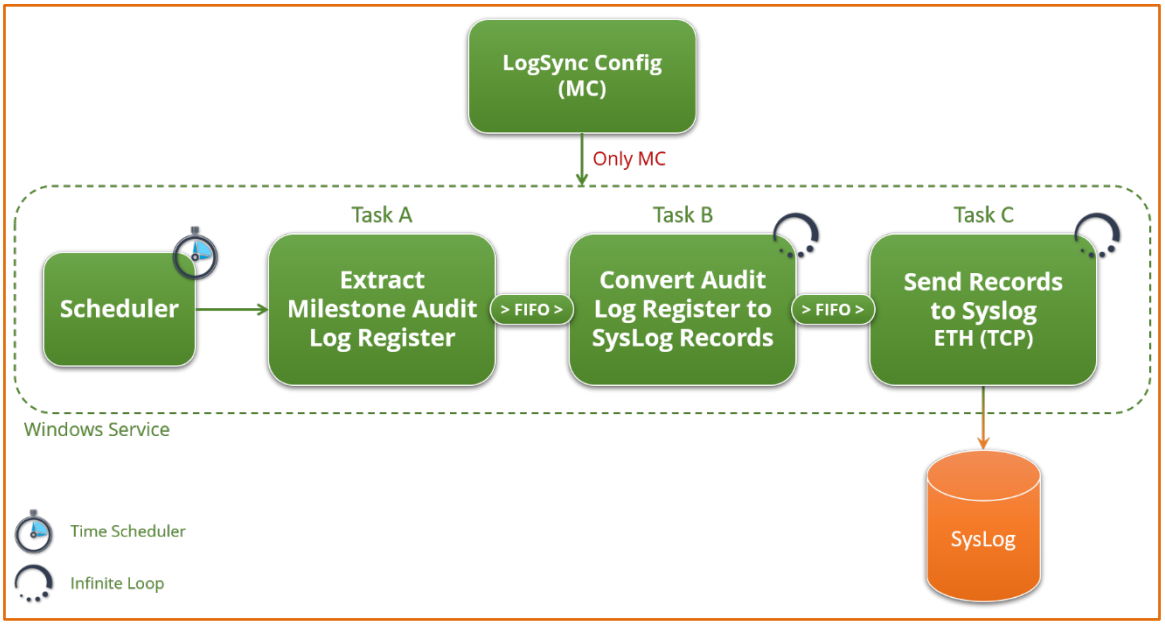
utilizzato dal Servizio. I messaggi di questo registro, oltre ad indicare se si verificano anomalie (Warning e/o Errori) consentono di verificare immediatamente se le schedulazioni avvengono con la cadenza prevista. Di seguito un esempio di tale Registro.



5.2 Servizio di Windows

Il Servizio di Windows non offre alcuna interazione con gli Utenti, è sempre residente in memoria ed è fondamentalmente composto da 3 task distinte, ciascuna con un compito specifico.

Lo schema di principio è illustrato nella figura seguente.



Occorre precisare che le 3 task, del tutto asincrone tra loro, si scambiano le informazioni utilizzando delle code di tipo FIFO per garantire che una eventuale interruzione della catena non crei problemi e, soprattutto, la perdita di messaggi da inviare al Server SysLog.

Per esempio, nel caso il Server SysLog non sia raggiungibile la Task C interromperà l'invio dei messaggi e la sua coda in entrata dalla Task B tenderà a riempirsi, quando questo avviene la Task B interromperà l'accodamento e sarà la sua coda in entrata che inizierà a riempirsi, quando anche questo accadrà sarà la Task A a non poter più accodare i messaggi, avendo però conservato le informazioni dell'ultimo messaggio accodato, quindi quando il funzionamento sarà ripristinato il primo messaggio che sarà accodato sarà proprio quello che non è stato possibile accodare la schedulazione precedente; lo stesso criterio è valido per le altre 2 task.

Il compito di ciascuna Task è il seguente:

- Task A: risulta essere normalmente ferma in attesa di essere attivata a intervalli prestabiliti dallo Scheduler Orario. Il compito specifico è leggere i messaggi di log presenti nel registro di XProtect, a partire dall'ultimo letto, di cui conserva le informazioni, e di accodarli nella FIFO verso la Task B
- Task B: risulta essere sempre attiva controllando costantemente la presenza di messaggi nella propria coda d'entrata, che elabora immediatamente. Il compito specifico è creare il record SysLog a partire da quello XProtect, per poi accodarlo nella FIFO verso la Task C

- Task C: come la precedente è sempre attiva e controlla la presenza di messaggi nella propria coda d'entrata. Il compito specifico è quello di inviare, utilizzando il protocollo TCP, i record al Server Syslog

Il compito delle code FIFO, oltre a quanto descritto in precedenza, è anche quello di rendere completamente asincrone tra loro le 3 task in modo tale che nessuna task sia costretta a dover attendere il completamento delle operazioni di quella a valle. Un esempio per chiarire: supponiamo che ad una data schedulazione siano presenti un migliaio di nuovi messaggi di log sulla Piattaforma XProtect, dopo un dato ritardo dovuto alla lettura la Task A inizierà ad accodare i messaggi, senza alcun tipo di ulteriore elaborazione, verso la Task B la quale, accorgendosi della presenza di messaggi nella coda inizierà ad elaborarli per poi accodarli verso la Task C. Poiché deve compiere delle elaborazioni per ciascun messaggio la Task B impiegherà più tempo della A, che dopo averli letti deve solo accodarli, quindi la prima FIFO inizierà a crescere. In assenza di interruzioni del collegamento dunque la Task A completerà il suo compito, tornando a riposo, quando ancora la Task B ha dei messaggi in coda da processare. Il funzionamento tra le Task B e C è del tutto analogo ma ancora più marcato poiché l'invio di un pacchetto su rete richiede più tempo di quanto necessiti l'elaborazione dello stesso da parte della Task B.

In pratica in condizioni nominali di funzionamento di seguito quello che accade:

- Tutto a riposo con le code vuote
- Avvio schedulazione: la Task A inizia l'accodamento dei messaggi che causa l'avvio delle attività della Task B, che a sua volta causa l'inizio della Attività della Task C
- La prima FIFO cresce, visto che l'accodamento richiede meno tempo dello scodamento da parte della Task B, inizia a crescere anche la FIFO della Task C che richiede ancora più tempo per lo scodamento
- La task A termina i propri accodamenti e torna a riposo
- La task B prosegue per dell'altro tempo fino a quando la sua coda d'entrata non risulta vuota e torna nello stato di attesa
- Stesso discorso per la Task C che impiegando più tempo della precedente sarà attiva per un altro periodo di tempo fino allo svuotamento della propria coda d'entrata
- L'intero Servizio si pone nello stato di attesa della schedulazione successiva

6 Licenza dell'Applicazione

La gestione della licenza d'uso dell'applicazione è conforme ai requisiti del Licensing Framework di Milestone, pertanto la specifica licenza rappresenta una estensione della licenza base della Piattaforma, definita SLC (Software License Code).

Lo schema di licensing è basato sul singolo Server (Site License).

SECURSYS