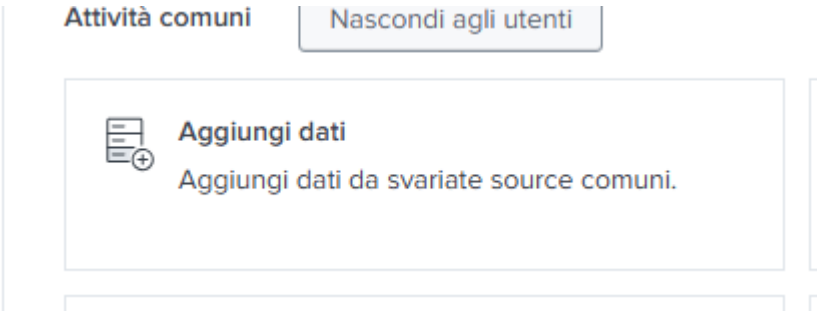
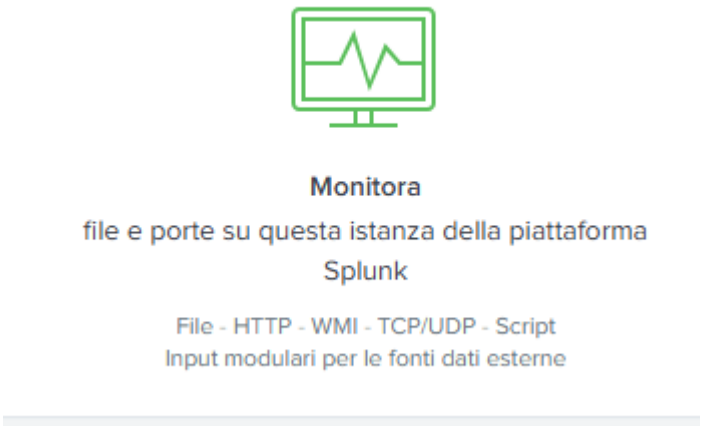
S10 L1 - SPLUNK
Esercizio

Configurare la modalità Monitora in Splunk

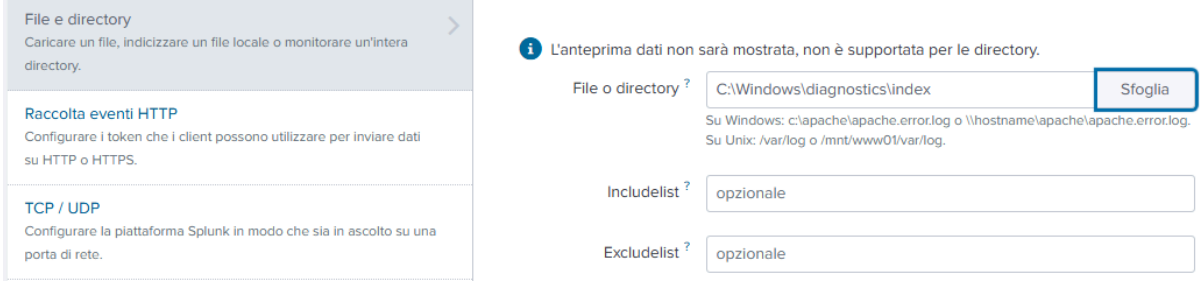
Aggiungi dati:



Monitora:

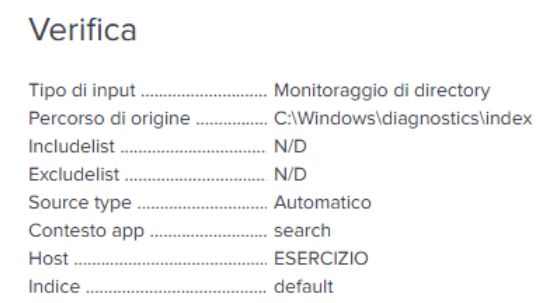


Selezionare il percorso della directory:

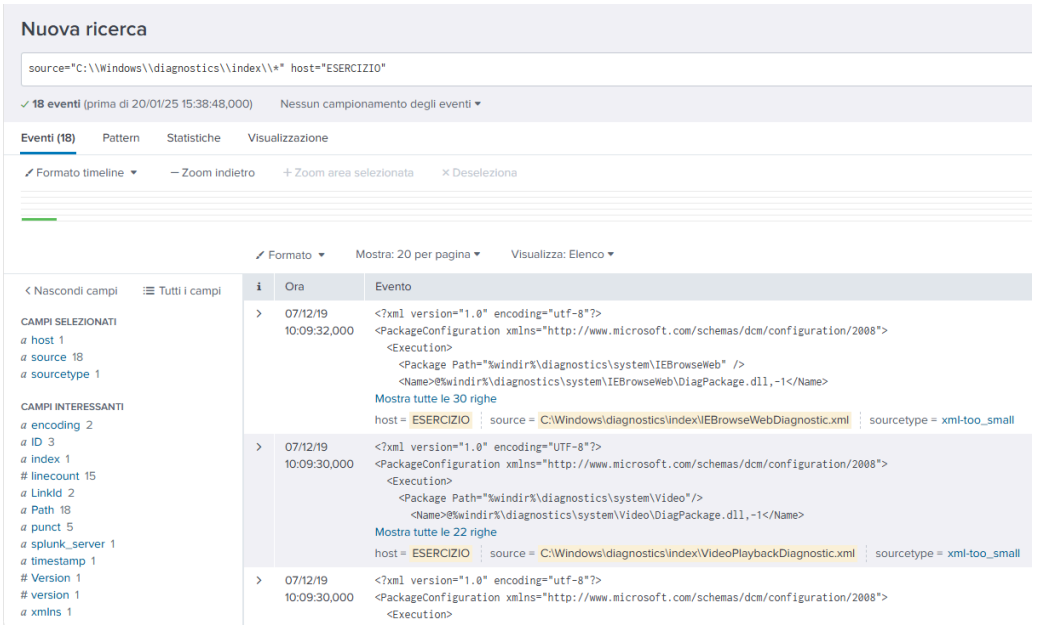


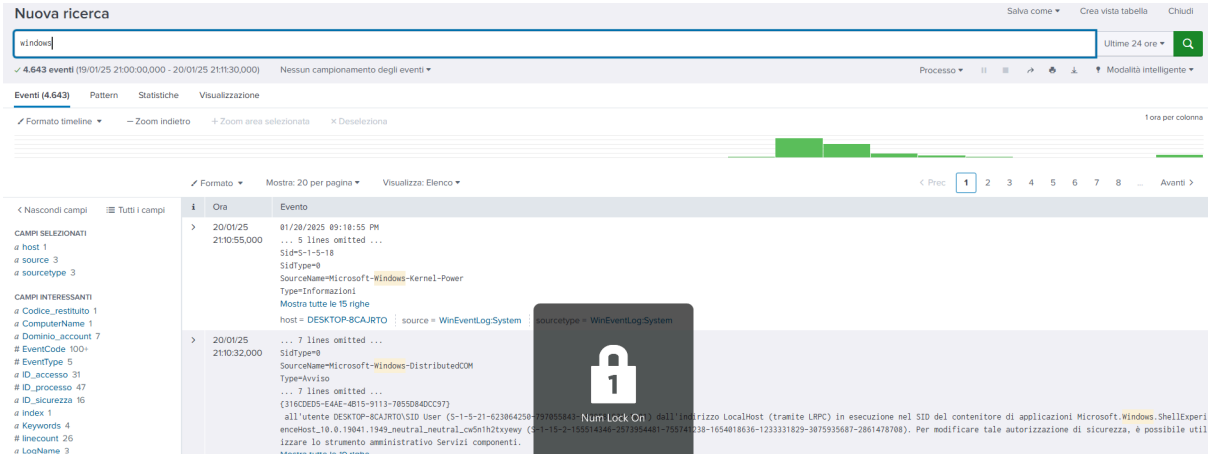
Configuro l' indirizzo IP per accettare la comunicazione solo da questo.
In questo caso non ha molto senso perché abbiamo una sola macchina collegata, ma in uno scenario con più dispositivi ha la sua utilità.

Una volta completata la configurazione verifica il recap.



Adesso siamo pronti per il monitoraggio




Nuova ricerca
Salva come
Crea vista tabella
Chiudi
windows
Ultime 24 ore
4.643 eventi (19/01/25 21:00:00,000 - 20/01/25 21:11:30,000)
Nessun campionamento degli eventi
Processo
Modalità intelligente
Eventi (4.643)
Pattern
Statistiche
Visualizzazione
Formato timeline
Zoom indietro
Zoom area selezionata
Deseleziona
1 ora per colonna
Formato
Mostra: 20 per pagina
Visualizza: Elenco
Prec
1
2
3
4
5
6
7
8
Avanti
Nascondi campi
Tutti i campi
CAMPI SELEZIONATI
host 1
source 3
sourcetype 3
CAMPI INTERESSANTI
Codice_restituito 1
ComputerName 1
Dominio_account 7
EventCode 100+
EventType 5
ID_accesso 31
ID_processo 47
ID_sicurezza 16
index 1
Keywords 4
linecount 26
LogName 3
Ora
Evento
20/01/25 21:10:55,000
01/20/2025 09:10:55 PM
... 5 lines omitted ...
Sid=S-1-5-18
SidType=0
SourceName=Microsoft-Windows-Kernel-Power
Type=Informazioni
Mostra tutte le 15 righe
host = DESKTOP-8CAJRTO
source = WinEventLog:System
sourcetype = WinEventLog:System
20/01/25 21:10:32,000
... 7 lines omitted ...
SidType=0
SourceName=Microsoft-Windows-DistributedCOM
Type=Avviso
... 7 lines omitted ...
{316CDED5-E4AE-4B15-9113-7055D84DCC97}
all'utente DESKTOP-8CAJRTO\SID User (S-1-5-21-623064250-797055843-
) dall'indirizzo LocalHost (tramite LRPC) in esecuzione nel SID del contenitore di applicazioni Microsoft.Windows.ShellExperienceHost_10.0.19041.1949_neutral_neutral_cw5n1h2txyewy (S-1-15-2-155514346-2573954481-755747238-1654018636-1233331829-3075935687-2861478708). Per modificare tale autorizzazione di sicurezza, è possibile utilizzare lo strumento amministrativo Servizi componenti.
Num Lock On