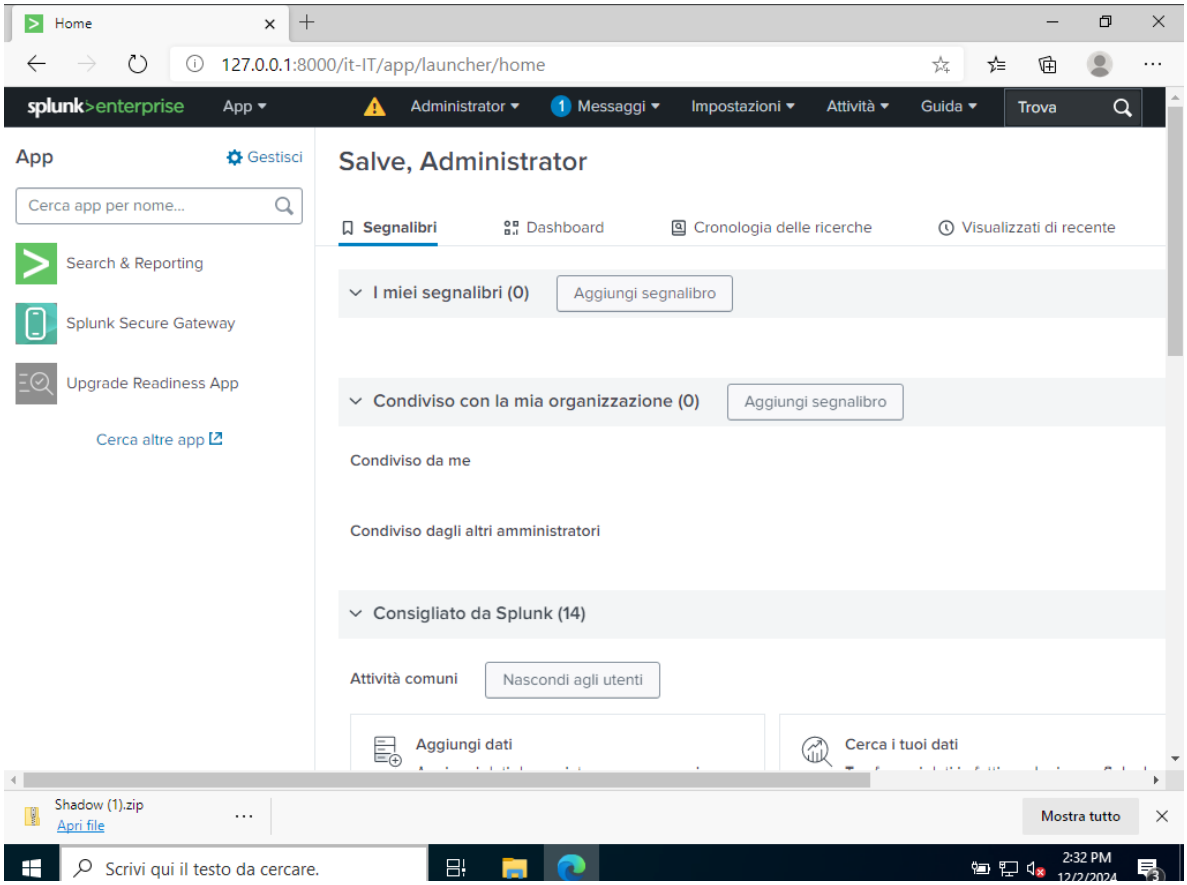
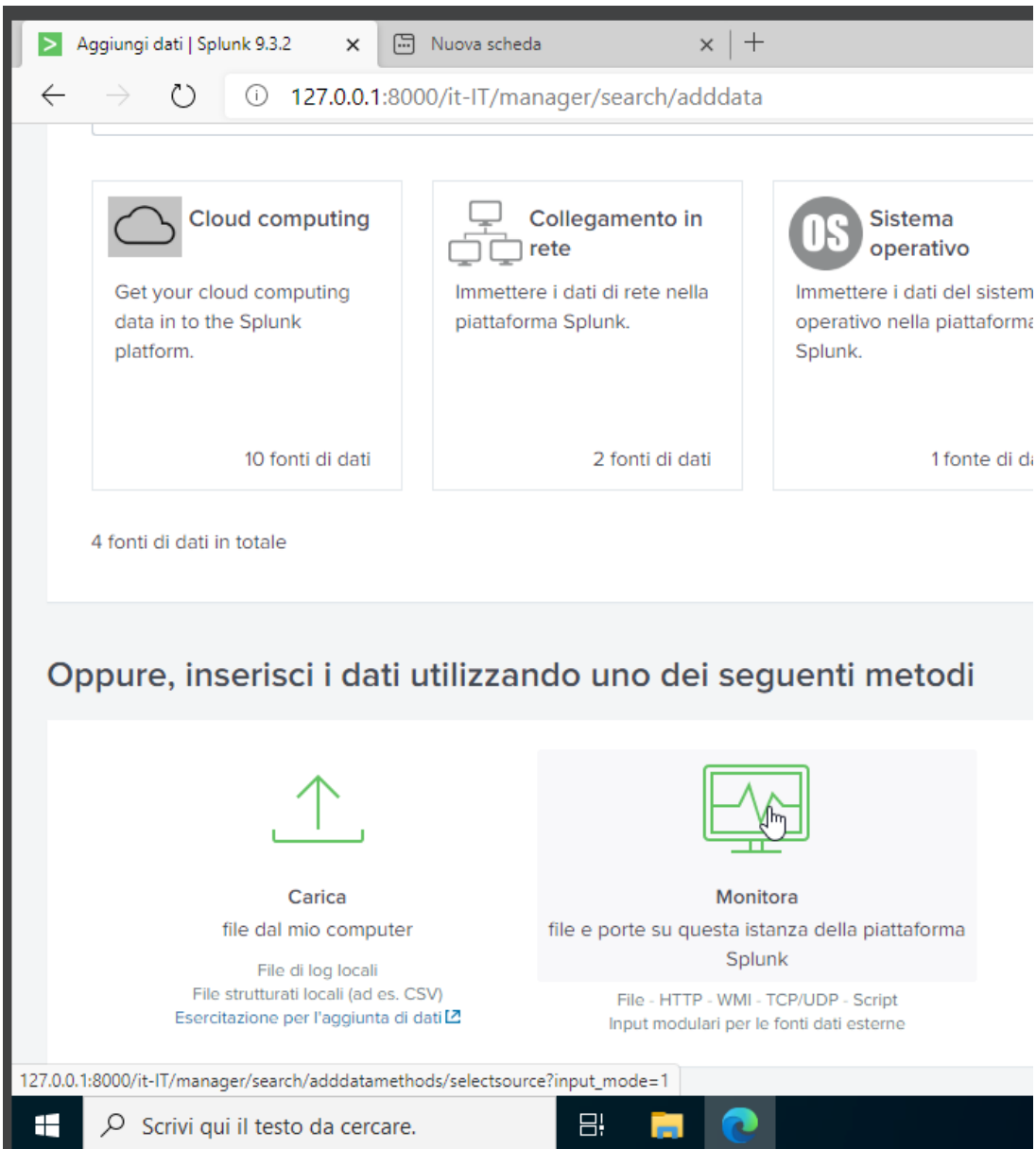
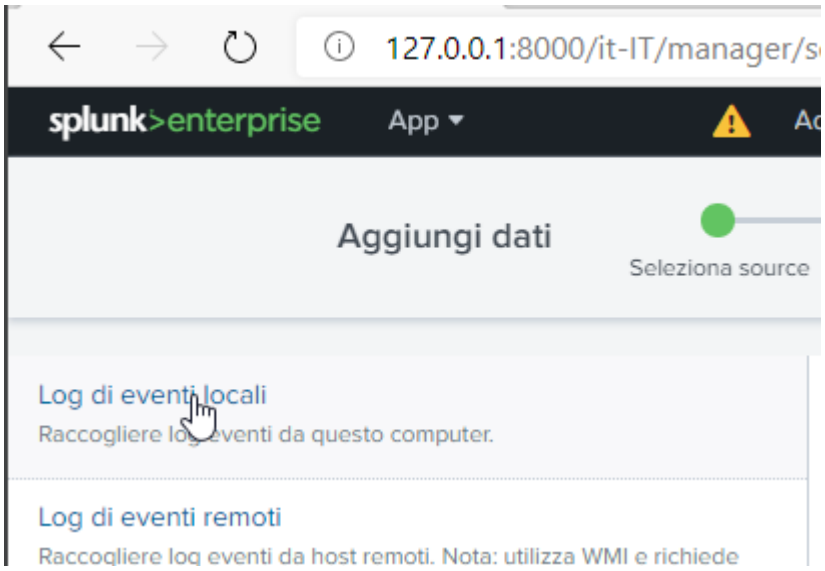
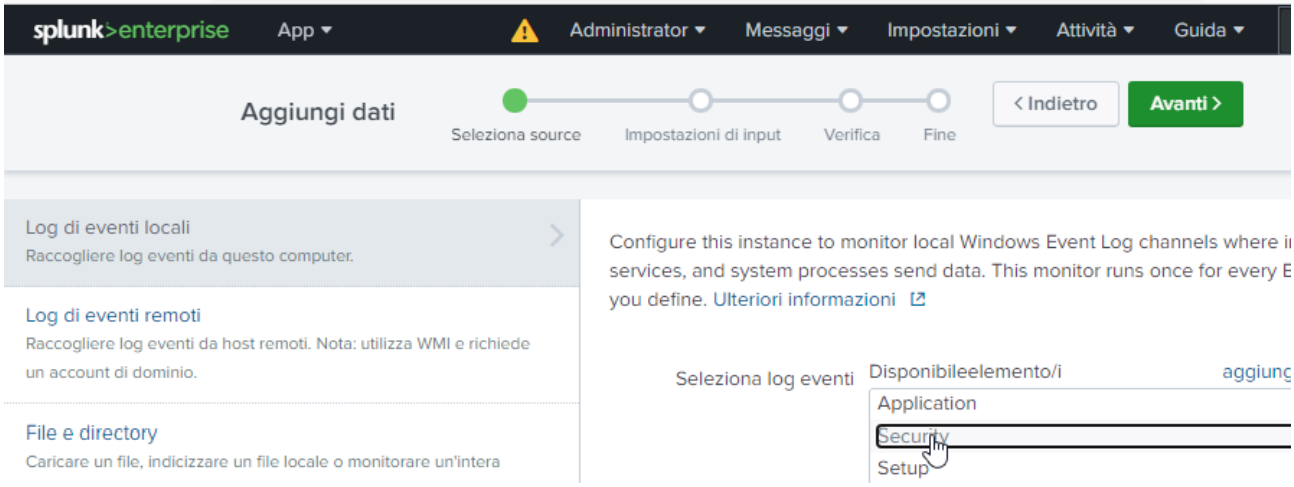
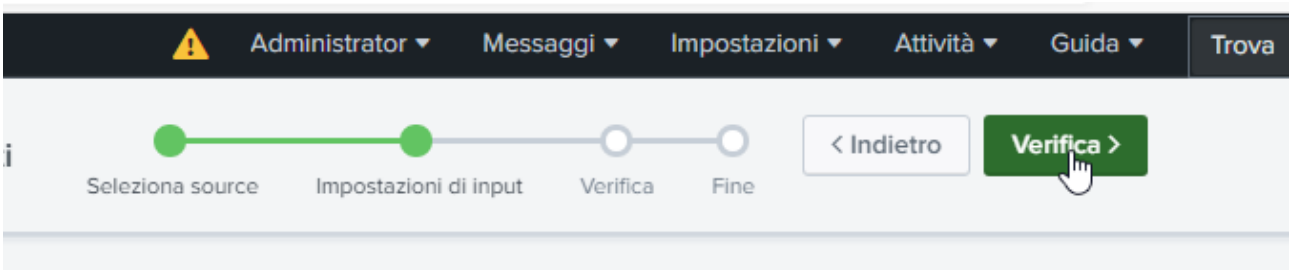
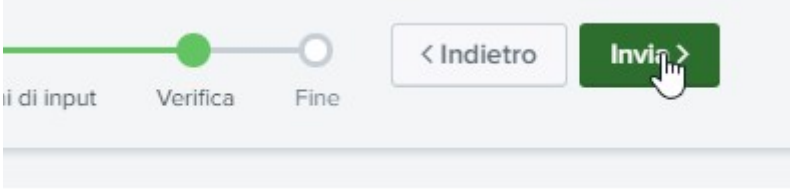

Home
127.0.0.1:8000/it-IT/app/launcher/home
splunk>enterprise
App
Administrator
1 Messaggi
Impostazioni
Attività
Guida
Trova
App
Gestisci
Cerca app per nome...
Search & Reporting
Splunk Secure Gateway
Upgrade Readiness App
Cerca altre app
Salve, Administrator
Segnalibri
Dashboard
Cronologia delle ricerche
Visualizzati di recente
I miei segnalibri (0)
Aggiungi segnalibro
Condiviso con la mia organizzazione (0)
Aggiungi segnalibro
Condiviso da me
Condiviso dagli altri amministratori
Consigliato da Splunk (14)
Attività comuni
Nascondi agli utenti
Aggiungi dati
Cerca i tuoi dati
Shadow (1).zip
Apri file
Mostra tutto
Scrivi qui il testo da cercare.
2:32 PM

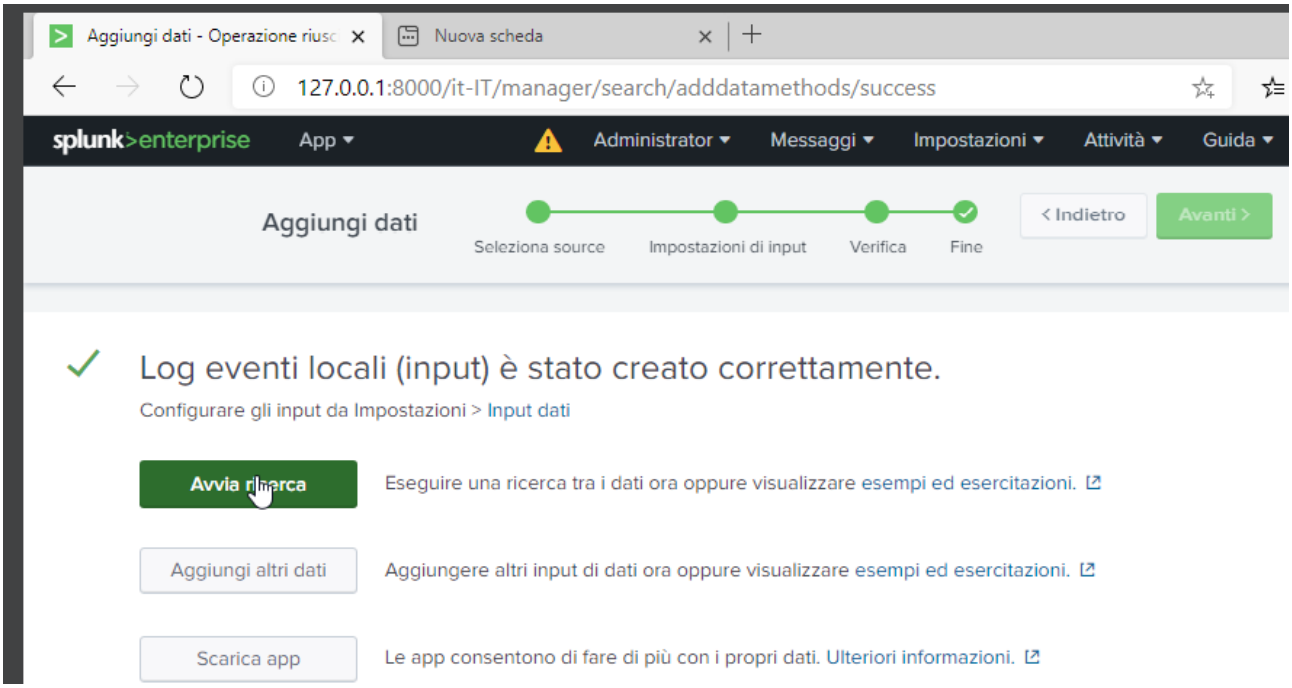

Aggiungi dati | Splunk 9.3.2
Nuova scheda
127.0.0.1:8000/it-IT/manager/search/adddata
Cloud computing
Get your cloud computing data in to the Splunk platform.
10 fonti di dati
Collegamento in rete
Immettere i dati di rete nella piattaforma Splunk.
2 fonti di dati
OS
Sistema operativo
Immettere i dati del sistem operativo nella piattaforma Splunk.
1 fonte di d
4 fonti di dati in totale
Oppure, inserisci i dati utilizzando uno dei seguenti metodi
Carica
file dal mio computer
File di log locali
File strutturati locali (ad es. CSV)
Esercitazione per l'aggiunta di dati
Monitora
file e porte su questa istanza della piattaforma Splunk
File - HTTP - WMI - TCP/UDP - Script
Input modulari per le fonti dati esterne
127.0.0.1:8000/it-IT/manager/search/adddatamethods/selectsource?input_mode=1
Scrivi qui il testo da cercare.

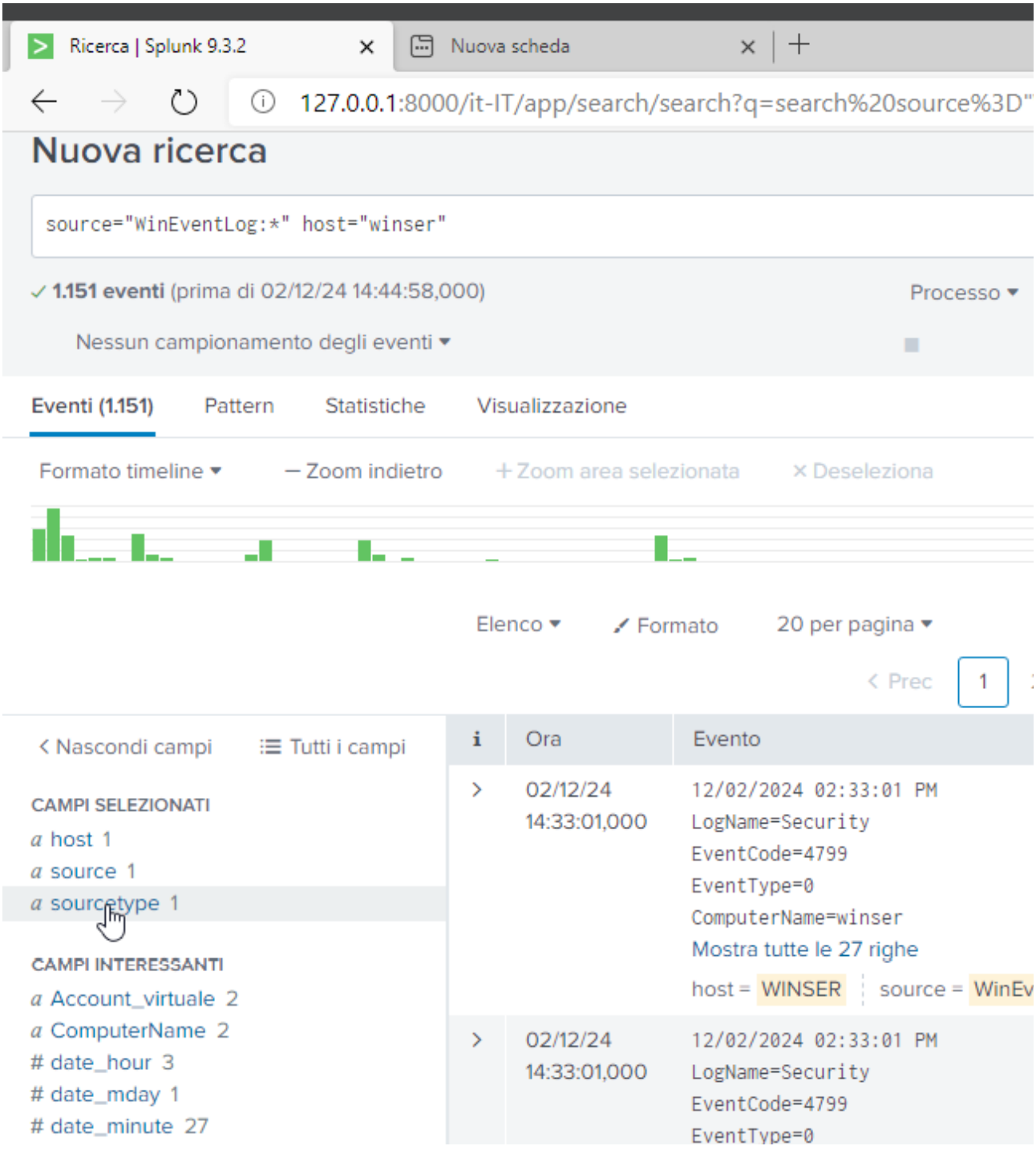

127.0.0.1:8000/it-IT/manager/s
splunk>enterprise
App
Aggiungi dati
Seleziona source
Log di eventi locali
Raccogliere log eventi da questo computer.
Log di eventi remoti
Raccogliere log eventi da host remoti. Nota: utilizza WMI e richiede


splunk>enterprise
App
Administrator
Messaggi
Impostazioni
Attività
Guida
Aggiungi dati
Seleziona source
Impostazioni di input
Verifica
Fine
< Indietro
Avanti >
Log di eventi locali
Raccogliere log eventi da questo computer.
Log di eventi remoti
Raccogliere log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.
File e directory
Caricare un file, indicizzare un file locale o monitorare un'intera
Configure this instance to monitor local Windows Event Log channels where i
services, and system processes send data. This monitor runs once for every E
you define. Ulteriori informazioni
Seleziona log eventi
Disponibileelemento/i
aggiung
Application
Security
Setup


Administrator
Messaggi
Impostazioni
Attività
Guida
Trova
Seleziona source
Impostazioni di input
Verifica
Fine
< Indietro
Verifica >


i di input
Verifica
Fine
< Indietro
Invia >


Aggiungi dati - Operazione riusc
Nuova scheda
127.0.0.1:8000/it-IT/manager/search/adddatamethods/success
splunk>enterprise
App
Administrator
Messaggi
Impostazioni
Attività
Guida
Aggiungi dati
Seleziona source
Impostazioni di input
Verifica
Fine
< Indietro
Avanti >
Log eventi locali (input) è stato creato correttamente.
Configurare gli input da Impostazioni > Input dati
Avvia ricerca
Eseguire una ricerca tra i dati ora oppure visualizzare esempi ed esercitazioni.
Aggiungi altri dati
Aggiungere altri input di dati ora oppure visualizzare esempi ed esercitazioni.
Scarica app
Le app consentono di fare di più con i propri dati. Ulteriori informazioni.


Ricerca | Splunk 9.3.2
Nuova scheda
127.0.0.1:8000/it-IT/app/search/search?q=search%20source%3D"
Nuova ricerca
source="WinEventLog:*" host="winser"
1.151 eventi (prima di 02/12/24 14:44:58,000)
Processo
Nessun campionamento degli eventi
Eventi (1.151)
Pattern
Statistiche
Visualizzazione
Formato timeline
Zoom indietro
Zoom area selezionata
Deseleziona
Elenco
Formato
20 per pagina
Prec
1
Nascondi campi
Tutti i campi
CAMPI SELEZIONATI
a host 1
a source 1
a sourcetype 1
CAMPI INTERESSANTI
a Account_virtuale 2
a ComputerName 2
date_hour 3
date_mday 1
date_minute 27
i
Ora
Evento
02/12/24 14:33:01,000
12/02/2024 02:33:01 PM
LogName=Security
EventCode=4799
EventType=0
ComputerName=winser
Mostra tutte le 27 righe
host = WINSER
source = WinEv
02/12/24 14:33:01,000
12/02/2024 02:33:01 PM
LogName=Security
EventCode=4799
EventType=0