

Dopo aver verificato che entrambe le macchine sono sulla stessa rete e comunicanti, verifichiamo che il servizio di Forwarding sia acceso:

Servizi (computer locale)					
Selezionare un elemento per visualizzarne la descrizione.					
Nome	Descrizione	Stato	Tipo di avvio	Con	
SplunkForwarder	SplunkForw...	In eseg...	Automatico	Siste	
Spooler di stampa	Questo serv...	In eseg...	Automatico	Siste	
Strumentazione gestione W...	Fornisce un ...	In eseg...	Automatico	Siste	
Strumento di aggiornament...	Imposta aut...		Disabilitato	Servi	
Supporto del pannello di co...	Questo serv...		Manuale	Siste	
SysMain	Mantiene e ...	In eseg...	Automatico	Siste	
Telefonia	Fornisce il s...		Manuale	Servi	
Temi	Consente la...	In eseg...	Automatico	Siste	
Trap SNMP	Riceve mess...		Manuale	Servi	

Il Forwarder è impostato sulla porta 9997, andiamo a mettere in ascolto il nostro server sulla stessa porta

Administrator

2 Messaggi

Impostazioni

Attività

Guida

Trova

Salva

Seg

Aggiungi dati

Console di monitoraggio

Cond

Cond

ricezione

Configura ricezione

Inoltro e ricezione

Configurare l'host per l'invio e la ricezione di dati.

Event type

Tag

Campi

Lookup

Interfaccia utente

Azioni di allarme

Ricerca avanzata

Tutte le configurazioni

Indici

Sommari di accelerazione report

Source type

Azioni di inserimento

AMBIENTE DISTRIBUITO

Clustering di indexer

Gestione forwarder

Ricevi dati

Configurare questa istanza per ricevere dati inoltrati da altre istanze.

Tipo

Azioni

Configura ricezione

+ Aggiungi nuovo/a

Ricevi dati

Inoltro e ricezione » Ricevi dati

Nuova porta di ricezione

Visualizzazione 1-1 di 1 elemento

filtro

25 per pagina

In ascolto su questa porta

Stato

Azioni

9997

Abilitato | Disabilita


Elimina

Torniamo sulla home e clicchiamo su Cerca i tuoi dati:


Consigliato da Splunk (14)

Attività comuni


Nascondi agli utenti




Aggiungi dati
Aggiungi dati da svariate source comuni.




Cerca i tuoi dati
Trasforma i dati in fatti con la ricerca Splunk.




Visualizza i tuoi dati
Crea dashboard che funzionano per i tuoi dati.




Gestisci gli allarmi
Gestire gli allarmi che monitorano i propri dati



Aggiungi membri del team
Aggiungi i membri del team alla piattaforma Splunk.



Gestisci autorizzazioni
Controlla chi ha accesso con i ruoli.




Configura dispositivi mobili
Accedi o gestisci i dispositivi mobili con ...

Usando un prompt come “windows” possiamo visualizzare le attività del nostro client su cui abbiamo installato il forwarder.

Nuova ricerca

Salva come ▾ Crea vista tabella Chiudi

windows

Ultimi 60 minuti ▾ 

✓ 948 eventi (14/10/24 13:29:00,000 - 14/10/24 14:29:09,000)

Processo ▾ || ↶ ↷ ⌵ ⌴ ⌵ Modalità intelligente ▾

Nessun campionamento degli eventi ▾

Eventi (948)

Pattern

Statistiche

Visualizzazione


Formato timeline ▾

— Zoom indietro

+ Zoom area selezionata

x Deseleziona

1 minuto per colonna



Elenco ▾

✍ Formato

20 per pagina ▾

< Prec

1

2

3

4

5

6

7

8

...

Avanti >

< Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

a source 4

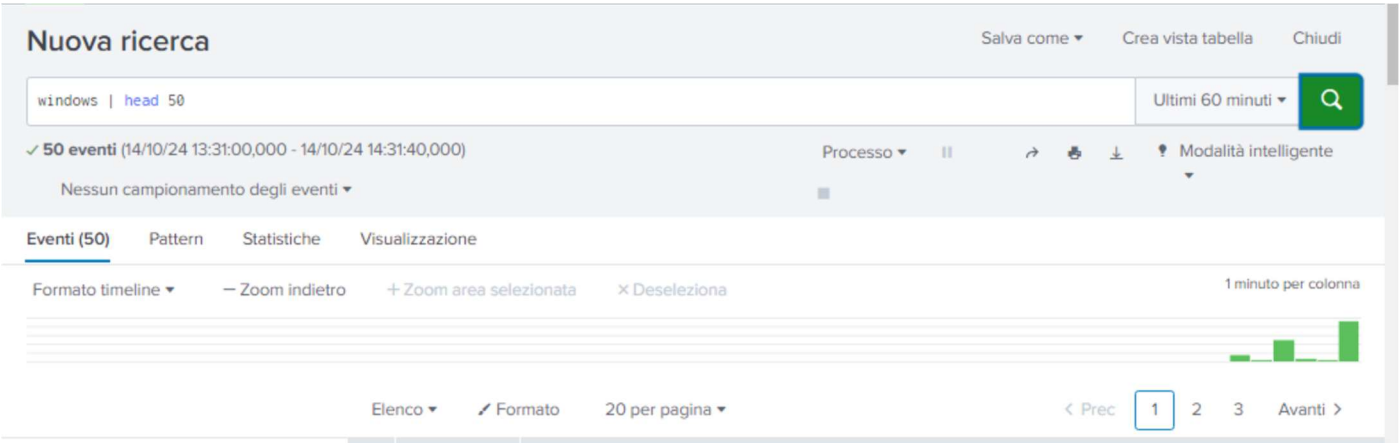
a sourcetype 4

CAMPI INTERESSANTI

a ComputerName 1

i	Ora	Evento
>	14/10/24 14:28:54,000	AddressFamily=ipv4 ... 9 lines omitted ... RemoteAddress=8.8.4.4 RemotePort=53 ProcessName="c:\windows\system32\svchost.exe" UserName="desktop-k9amt40\$" Mostra tutte le 19 righe host = DESKTOP-K9AMT40 source = Test sourcetype = WinNetMon

Usando come prompt windows | head 50 ci verranno visualizzati gli ultimi 50 risultati



Possiamo usare la colonna a sinistra per popolare la nostra query e cercare risultati specifici:

< Nascondi campi

CAMPI SELEZIONATI

Tutti i campi

a host 1

a Protocol 1

a source 1

a sourcetype 1

CAMPI INTERESSANTI

a AddressFamily 2

AddressFamilyId 2

a Direction 1

HeaderSizeBytes 1

a index 1

IPsecProtected 1

linecount 1

a LocalAddress 3

LocalPort 100+

a PacketType 1

PacketTypeId 1

a ProcessName 1

ProtocolId 1

a punct 6

a RemoteAddress 7

a RemoteHostName 5

RemotePort 4

a splunk_server 1

a timestamp 1

TransportHeaderSizeBytes 1

a UserId 2

a UserName 2

a UserSid 2

+ Estrai nuovi campi

Ad esempio, possiamo popolare la query in modo specifico da ritornarci un risultato:

Nuova ricerca

Salva comeCrea vista tabellaChiudi

"error" | search sourcetype=access_combined_wcookie req_time="13/Oct/2024:08:16:21"

Ultimi 30 giorni

Q

✓ 1 evento (14/09/24 00:00:00,000 - 14/10/24 15:46:48,000)

Processo

Modalità intelligente

Nessun campionamento degli eventi

Eventi (1)

Pattern

Statistiche

Visualizzazione

Formato timeline

Zoom indietro

Zoom area selezionata

Deseleziona

1 giorno per colonna

Elenco

Formato

20 per pagina

< Nascondi campi

CAMPI SELEZIONATI

Tutti i campi

a host 1

a source 1

a sourcetype 1

CAMPI INTERESSANTI

i	Ora	Evento
>	13/10/24 08:16:21,000	209.160.24.63 - - [13/Oct/2024:08:16:21] "POST /cart/error.do?msg=NothingInCart&JSESSIONID=SD1SL10FF9ADFF50311 HTTP 1.1" 200 713 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-16" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3" 872 host = DESKTOP-K9AMT40 source = tutorialdata.zip:\www3\access.log sourcetype = access_combined_wcookie