

S10 L1 - SPLUNK

Esercizio

Configurare la modalità Monitora in Splunk

Aggiungi dati:

Attività comuni

Nascondi agli utenti



Aggiungi dati

Aggiungi dati da svariate source comuni.

Monitora:



Monitors

file e porte su questa istanza della piattaforma
Splunk

File - HTTP - WMI - TCP/UDP - Script
Input modulari per le fonti dati esterne

Selezionare il percorso della directory:

File e directory

Caricare un file, indicizzare un file locale o monitorare un'intera directory.

Raccolta eventi HTTP

Configurare i token che i client possono utilizzare per inviare dati su HTTP o HTTPS.

TCP / UDP

Configurare la piattaforma Splunk in modo che sia in ascolto su una porta di rete.

L'anteprima dati non sarà mostrata, non è supportata per le directory.

File o directory ?

C:\Windows\diagnostics\index

Sfoglia

Su Windows: c:\apache\apache.error.log o \\hostname\apache\apache.error.log.
Su Unix: /var/log o /mnt/www01/var/log.

Includelist ?

opzionale

Excludelist ?

opzionale

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.

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 directory.

Raccolta eventi HTTP

Configurare i token che i client possono utilizzare per inviare dati su HTTP o HTTPS.

TCP / UDP

Configurare la piattaforma Splunk in modo che sia in ascolto su una porta di rete.

TCP

UDP

Porta ?

9997

Esempio: 514

Sostituzione nome source ?

opzionale

host:porta

Accetta la connessione solo da ?

192.168.4.150

esempio: 10.1.2.3, !badhost.splunk.com, *.splunk.com

Una volta completata la configurazione verifica il recap.

Verifica

Tipo di input Monitoraggio di directory
Percorso di origine C:\Windows\diagnostics\index
Includelist N/D
Excludelist N/D
Source type Automatico
Contesto app search
Host ESERCIZIO
Indice default

Adesso siamo pronti per il moitoraggio

Nuova ricerca

source="C:\Windows\diagnostics\index*" host="ESERCIZIO"

✓ 18 eventi (prima di 20/01/25 15:38:48,000) Nessun campionamento degli eventi ▼

Eventi (18)

Pattern

Statistiche

Visualizzazione

✓ Formato timeline ▼ — Zoom indietro + Zoom area selezionata × Deseleziona

✓ Formato ▼ Mostra: 20 per pagina ▼ Visualizza: Elenco ▼

< Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

a host 1

a source 18

a sourcetype 1

CAMPI INTERESSANTI

a encoding 2

a ID 3

a index 1

linecount 15

a Linkld 2

a Path 18

a punct 5

a splunk_server 1

a timestamp 1

Version 1

version 1

a xmlns 1

i

Ora

Evento

>

07/12/19 10:09:32,000

<?xml version="1.0" encoding="utf-8"?>
<PackageConfiguration xmlns="http://www.microsoft.com/schemas/dcm/configuration/2008">
<Execution>
<Package Path="%windir%\diagnostics\system\IEBrowseWeb" />
<Name>%windir%\diagnostics\system\IEBrowseWeb\DiagPackage.dll,-1</Name>
Mostra tutte le 30 righe
host = ESERCIZIO | source = C:\Windows\diagnostics\index\IEBrowseWebDiagnostic.xml | sourcetype = xml-too_small

>

07/12/19 10:09:30,000

<?xml version="1.0" encoding="UTF-8"?>
<PackageConfiguration xmlns="http://www.microsoft.com/schemas/dcm/configuration/2008">
<Execution>
<Package Path="%windir%\diagnostics\system\Video"/>
<Name>%windir%\diagnostics\system\Video\DiagPackage.dll,-1</Name>
Mostra tutte le 22 righe
host = ESERCIZIO | source = C:\Windows\diagnostics\index\VideoPlaybackDiagnostic.xml | sourcetype = xml-too_small

>

07/12/19 10:09:30,000

<?xml version="1.0" encoding="utf-8"?>
<PackageConfiguration xmlns="http://www.microsoft.com/schemas/dcm/configuration/2008">
<Execution>

