Day 30 -Troubleshooting

Troubleshooting

Terminato il progetto qui di seguito riassumo i casi più comuni di Troubleshooting e come sono stati affrontati.
Per i dettagli è possibile consultare gli elaborati dei Day precedenti di riferimento.

Connessione a Elastic/Kibana:

- Controllare le regole del firewall sul cloud provider (es. Vultr).
- Verificare le regole del firewall a livello di sistema operativo.
- Controllare lo stato dei servizi (ElasticSearch e Kibana).

Connessioni Fleet Server:

- Reinstallare l'agent sul Fleet Server per ripristinare la connessione.
- Modificare il firewall sul server ELK per garantire le connessioni necessarie.

Troubleshooting

Richiesta verso Fleet Server fallita:

- Verificare la documentazione sul sito Elastic per identificare le porte utilizzate nella comunicazione tra l'agent e il Fleet Server.

- Modificare la configurazione delle porte del Fleet Server per includere la porta **8220**, utilizzata dagli agenti su altre macchine (es. Windows).

- Verificare le regole del firewall del sistema operativo del Fleet Server, in particolare su porta 443.Da Kibana, accedere alla sezione Fleet e verificare l'URL utilizzato dagli agenti per la connessione al Fleet Server. Di default, l'URL è impostato su 443, ma è necessario modificarlo a 8220 per la corretta configurazione. Questa modifica deve riflettersi anche nella stringa di installazione dell'agent (ad esempio, quando si esegue l'installazione via PowerShell su Windows).Se necessario, aggiungere l'opzione --insecure per bypassare eventuali problemi di certificato(non essendo ambiente di produzione non è necessario).

Troubleshooting

Problema con agent che risulta "N/A" su Kibana:
Questo può indicare un problema con la porta **9200**, utilizzata per le comunicazioni di ElasticSearch. Verificare e modificare le regole del firewall per consentire il traffico su questa porta.

Problema di connessione del server remoto (Mythic Agent):
Verificare le regole del firewall sia del cloud provider che del sistema operativo per garantire che non vi siano blocchi che impediscono la connessione remota.