Contents

[DDoS Protection 1](#_Toc71115247)

[Yleinen 1](#_Toc71115248)

[Virtuaaliverkko 1](#_Toc71115249)

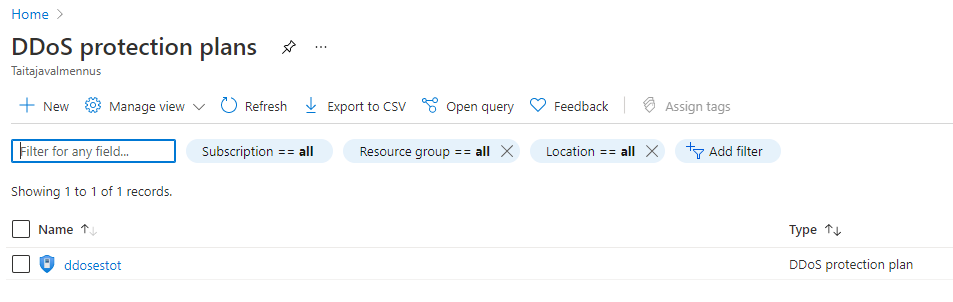
[Azure Sentinel 2](#_Toc71115250)

# DDoS Protection

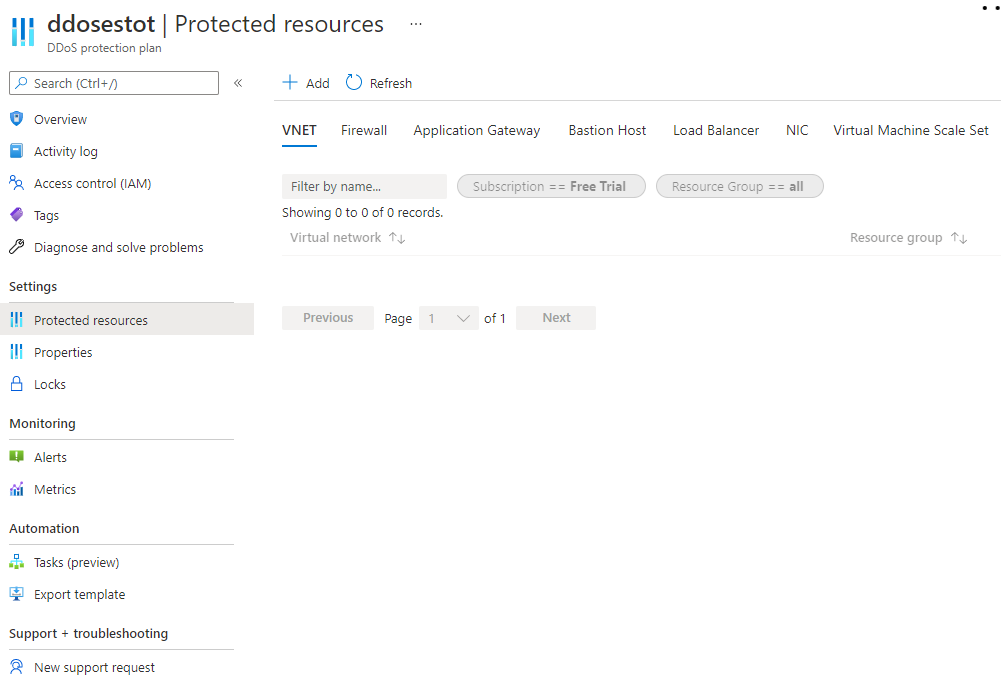
**Huom! Tämä maksaa paljon, joten älä ota käyttöön alkuvaiheissa!**

## Yleinen

DDoS Protection voit ehkäistä palvelunestohyökkäyksiä. Lisää uusi.

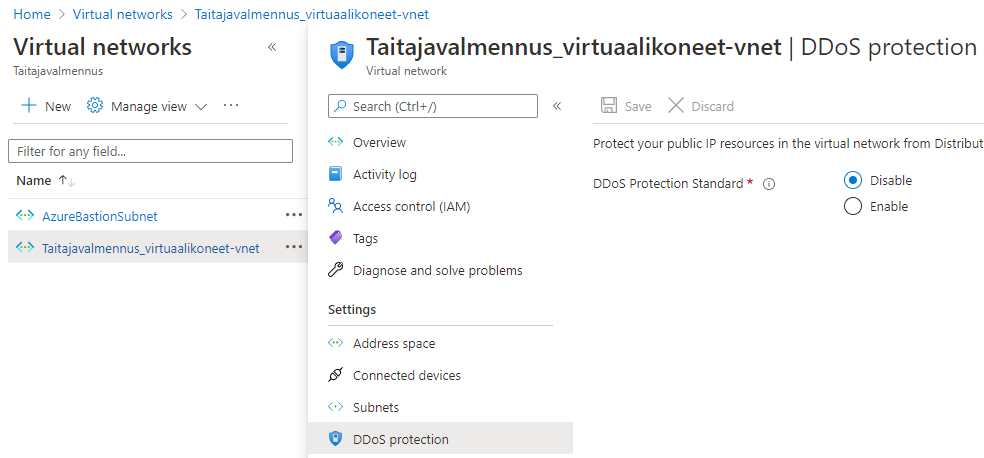


Määritä mitä haluat suojata DDoS hyökkäyksiltä. Esimerkiksi virtuaalikoneet.



## Virtuaaliverkko

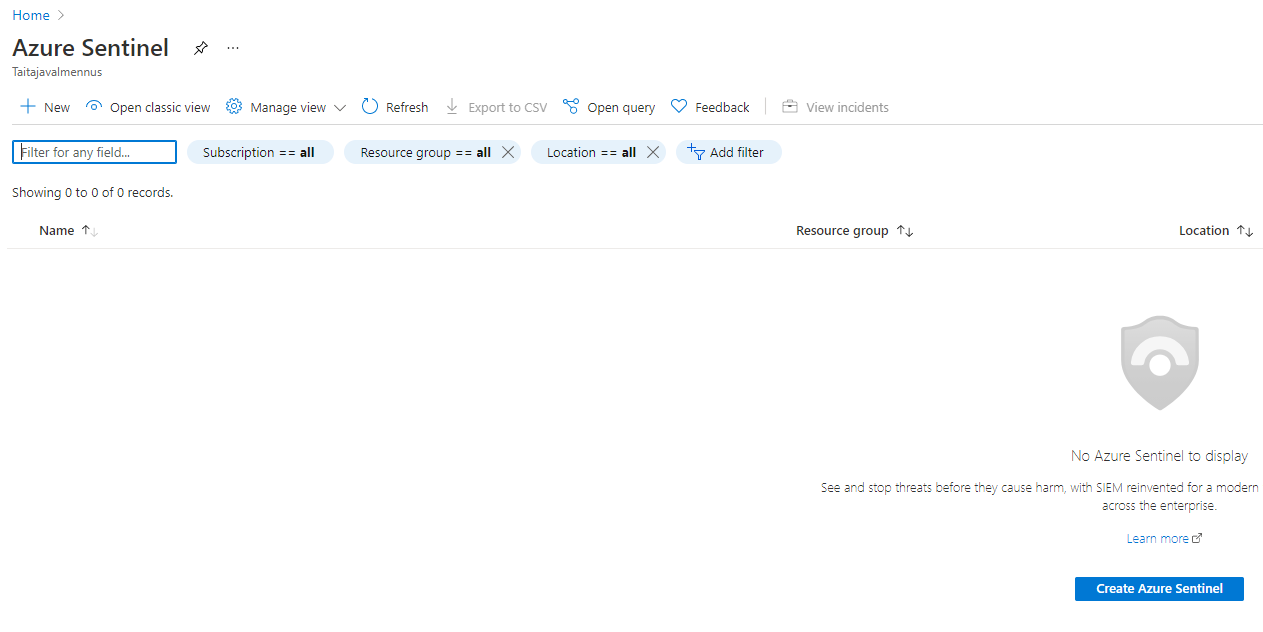
Tässä suojataan virtuaaliverkko palvelunestohyökkäykseltä.



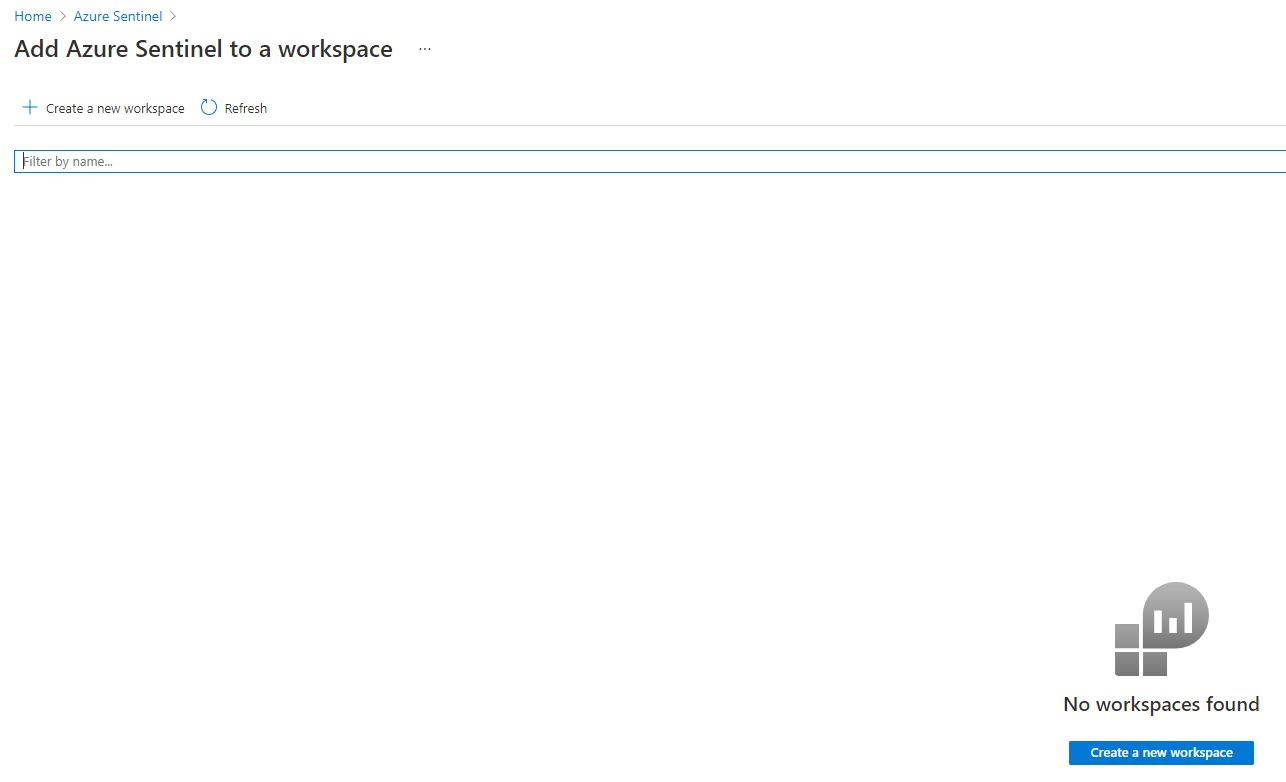
# Azure Sentinel

Azure Sentinel on Azuressa toimiva SIEM palvelu. SIEM on seurantatyökalu, johon kerätään tietoturvaan liittyviä tietoja eri palveluista.

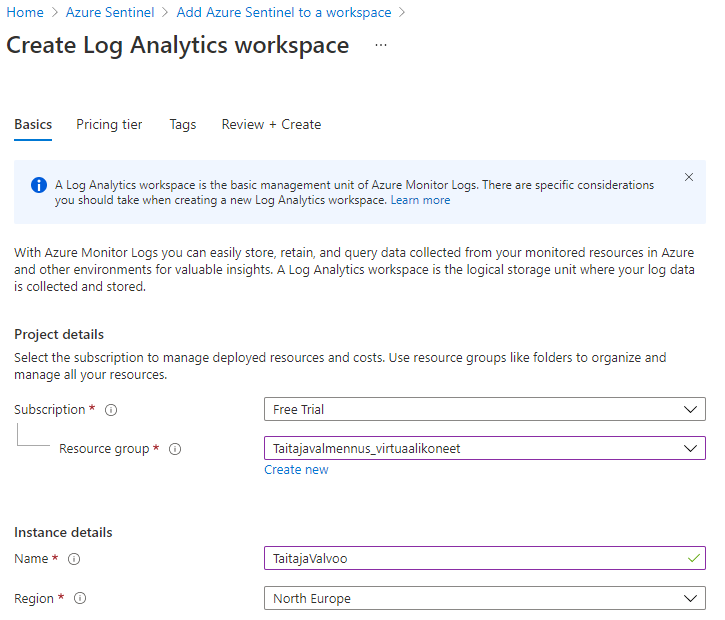
Ota käyttöön Sentinel ja luo uusi.



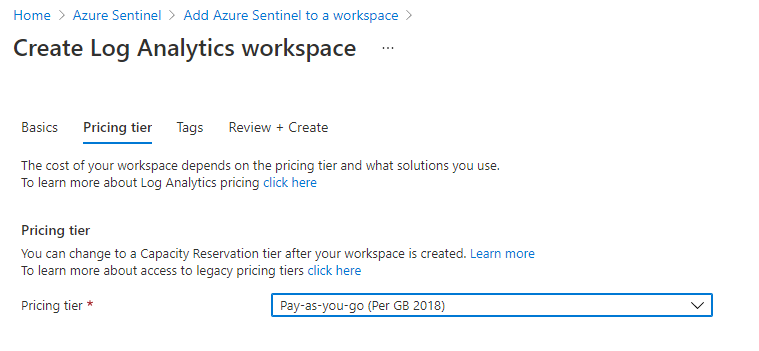
Luo Sentineliä varten uusi työtila.



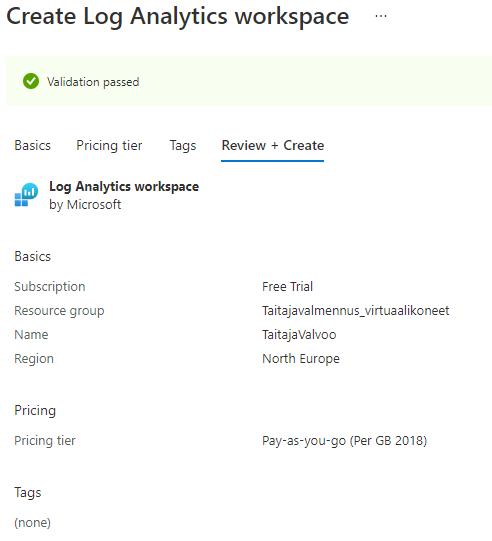
Joudut myös luomaan uuden Log Analytics työtilan, jotta lokeja voidaan käsitellä.



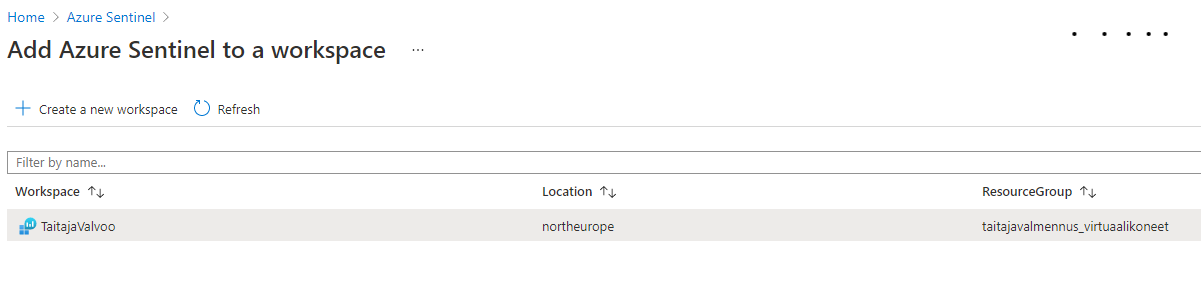
Määritetään miten laskutus hoidetaan.



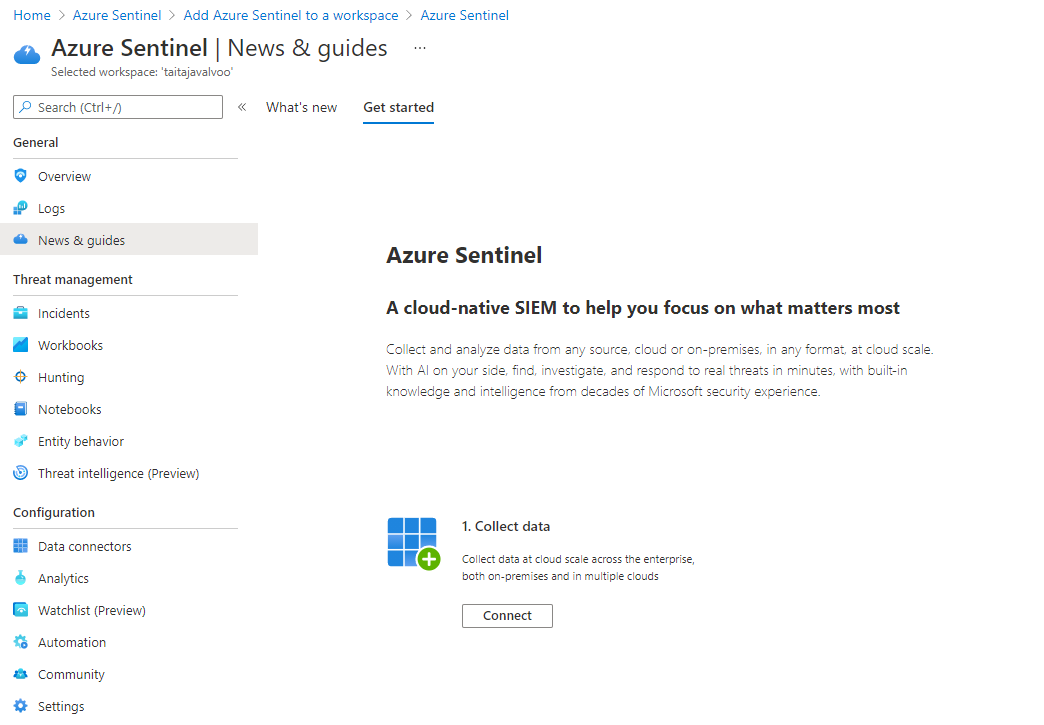
Yhteenveto ja luonti.



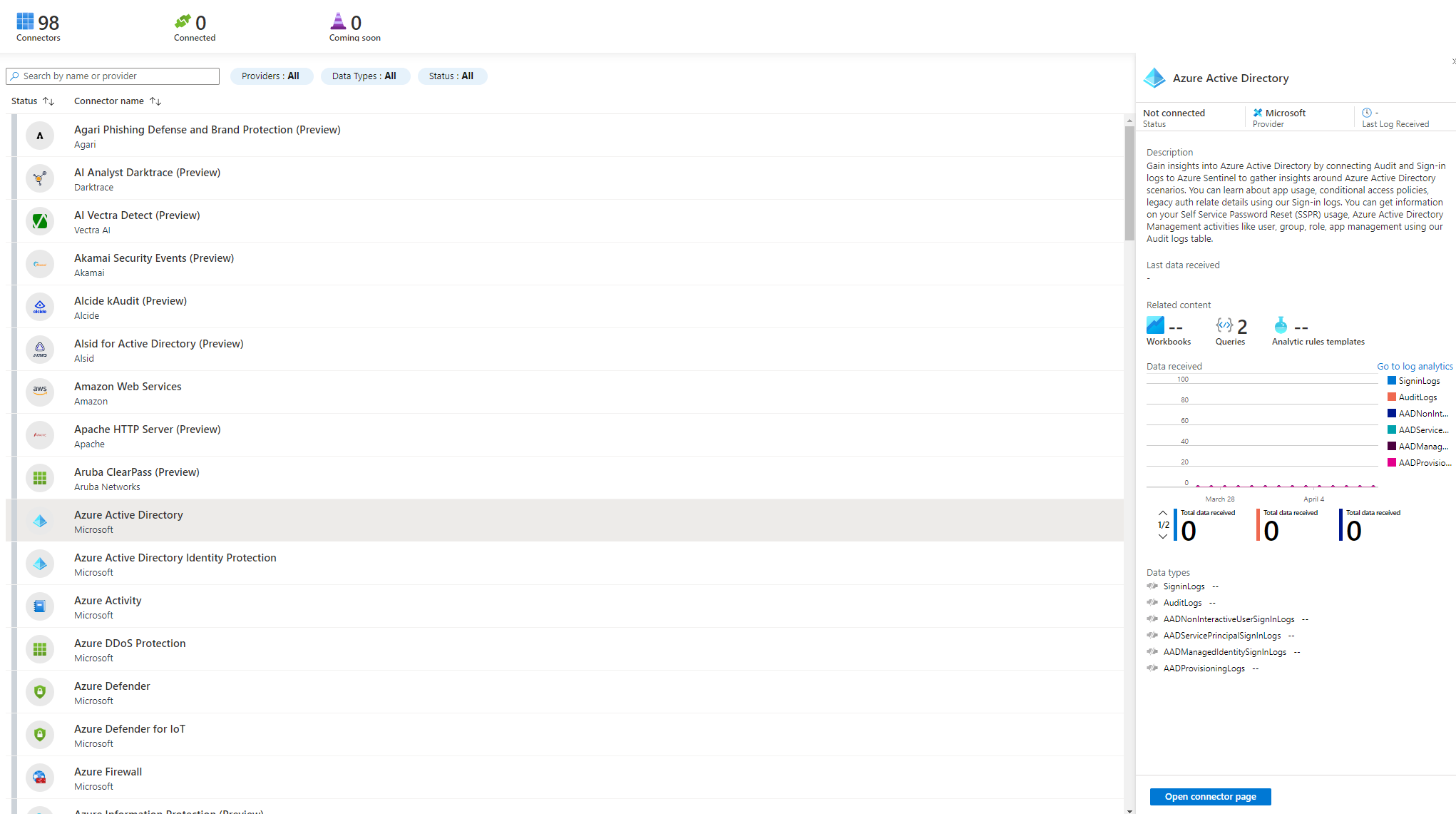
Azure Sentinel on nyt lisätty TaitajaValvoo työtilaan.



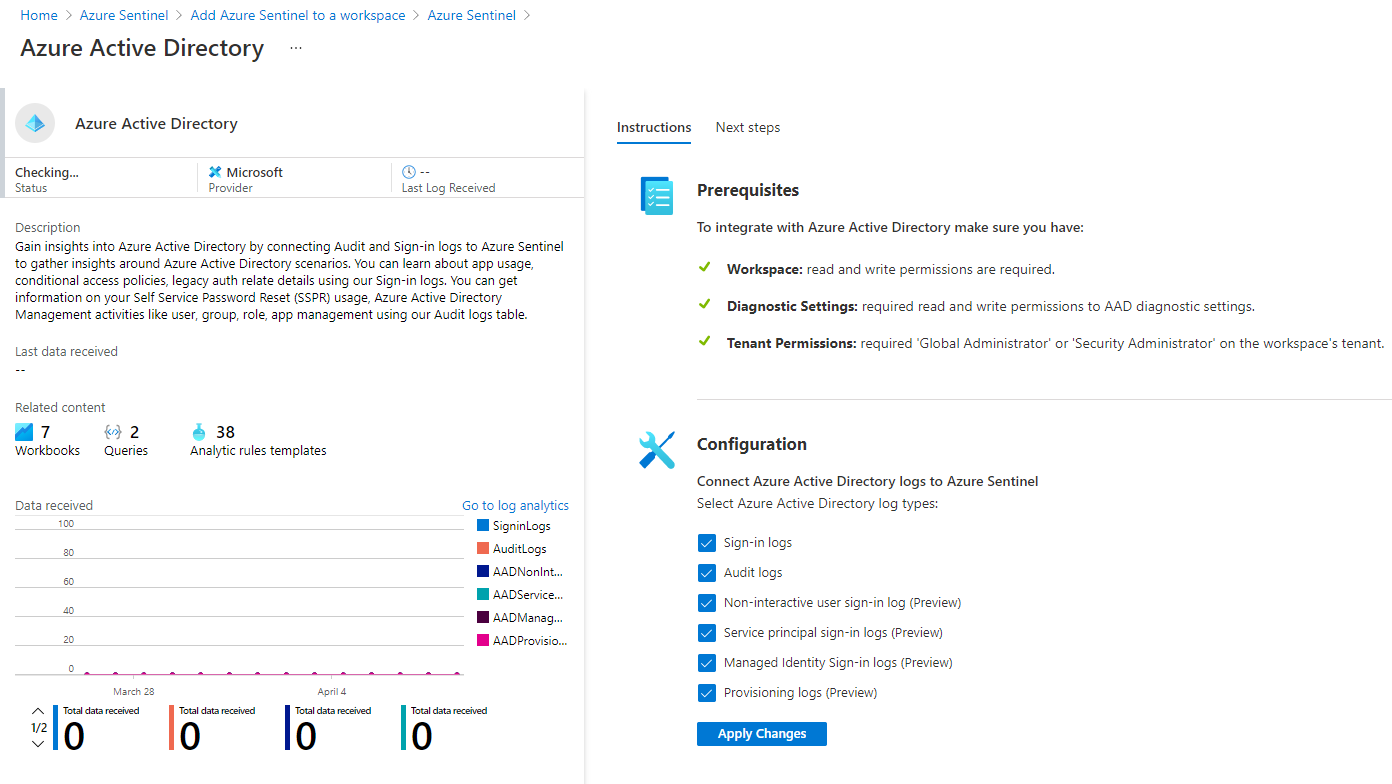
Sentineliin tulee tuoda dataa jostakin. Paina Connect painiketta.



Haetaan data meidän Azure AD:sta. Valitse Azure Active Directory ja sitten oikealta Open connector page.



Määritä Configuration kohtaan kaikki ja Apply changes.



Työtilaan tulee vielä tehdä työkirja johonkin malliin perustuen.

