Contents

[Virtuaalikoneet 1](#_Toc97187175)

[Windows 1](#_Toc97187176)

[Linux 8](#_Toc97187177)

[Hardened VMs 11](#_Toc97187178)

[Lisäosat (Extension) 11](#_Toc97187179)

[Virtuaaliverkot 11](#_Toc97187180)

[Network Security Groups (NSG) 12](#_Toc97187181)

[Diagram 13](#_Toc97187182)

[Yhteys virtuaalikoneeseen 13](#_Toc97187183)

[RDP 13](#_Toc97187184)

[SSH 17](#_Toc97187185)

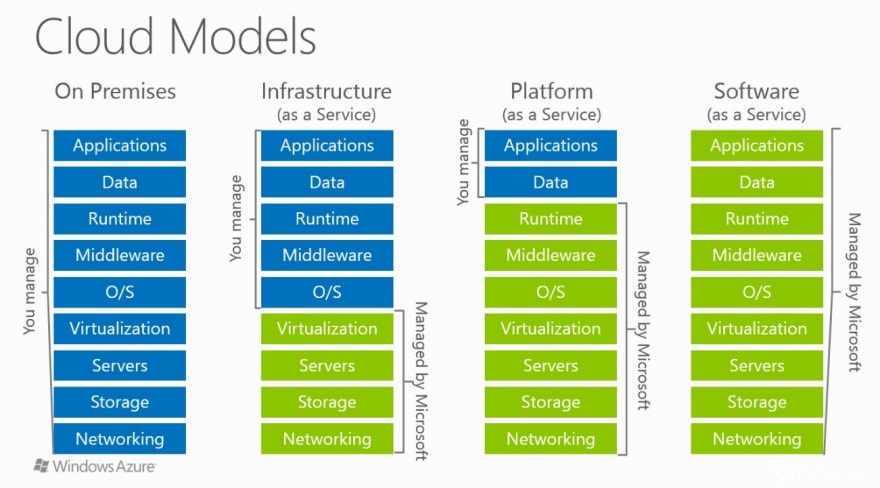
[Just-in-time (JIT) 19](#_Toc97187186)

[Bastion 22](#_Toc97187187)

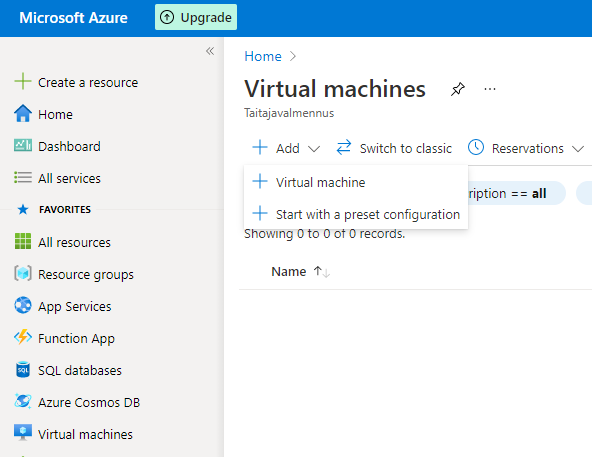
[Virtuaalikiintolevyjen salaaminen 27](#_Toc97187188)

# Virtuaalikoneet

Azureen voidaan luoda erilaisia virtuaalikoneita sen sijaan, että niitä ajettaisiin fyysisellä palvelimella oman yrityksen tiloissa. Virtuaalikoneet ovat IaaS tyyppinen pilvipalvelu eli sinun vastuullesi jää kaikki käyttöjärjestelmästä ylöspäin ja pilvipalvelu hoitaa esimerkiksi taustalla olevat rautapalvelimet ja virtualisoinnin.



Azuresta löytyy täysin oma osionsa virtuaalikoneille. Kuvan mukaisesti pääset luomaan uuden virtuaalikoneen.



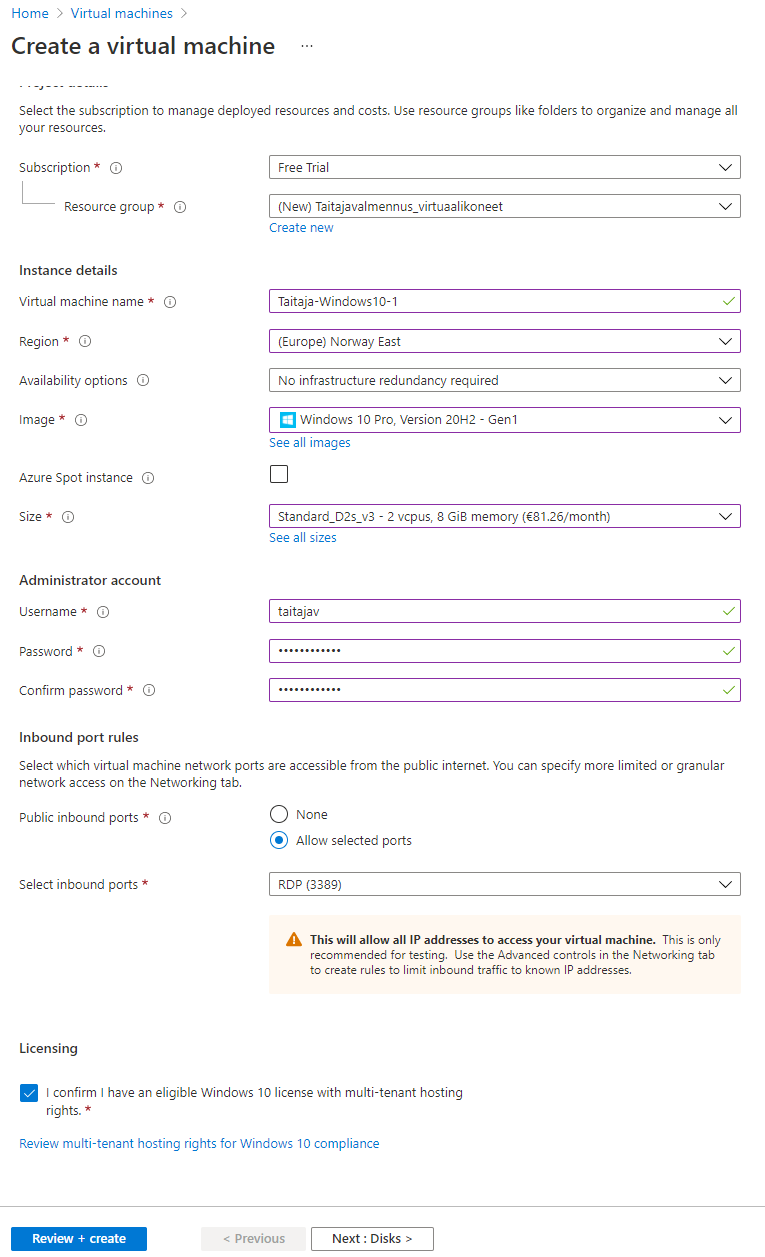
## Windows

Seuraavaksi määrität mihin Resource grouppiin tämä tehdään. Voit myös luoda uuden.

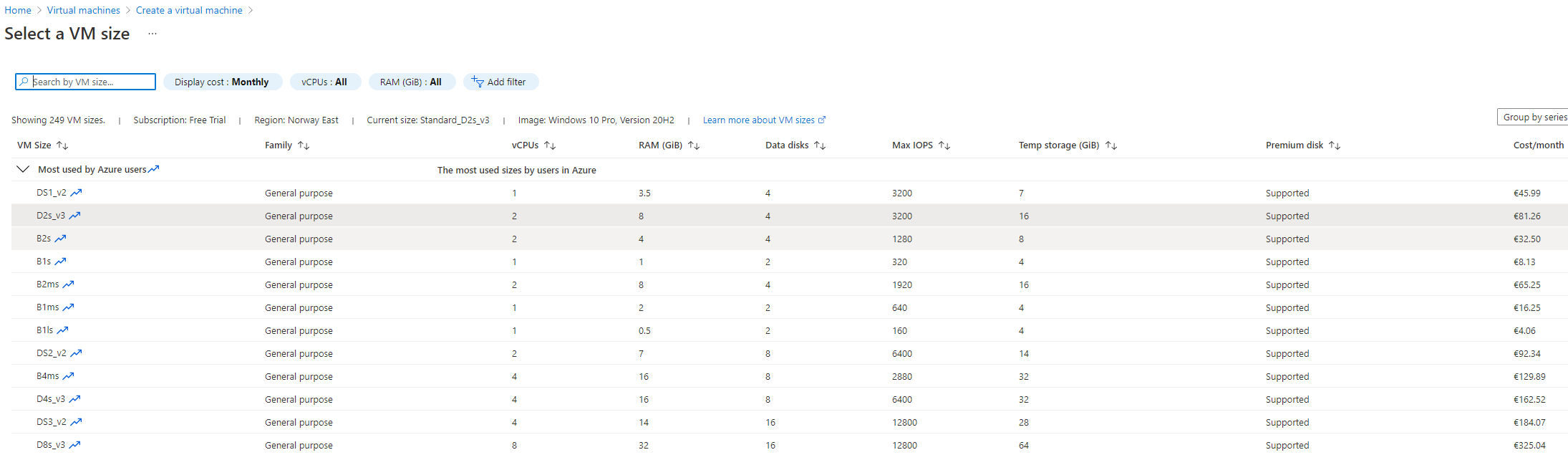
Anna virtuaalikoneelle nimi, alue (jossa datacenter sijaitsee, tässä Norjassa), miltä levykuvalta se luodaan (tässä Windows 10 Pro), valitse virtuaalikoneen resurssit (Size – tästä erillinen kuva alempana).

Sitten määritä virtuaalikoneen käyttäjätunnus ja salasana sekä miten siihen muodostetaan yhteys (tässä Remote Desktop) portin 3389 kautta.

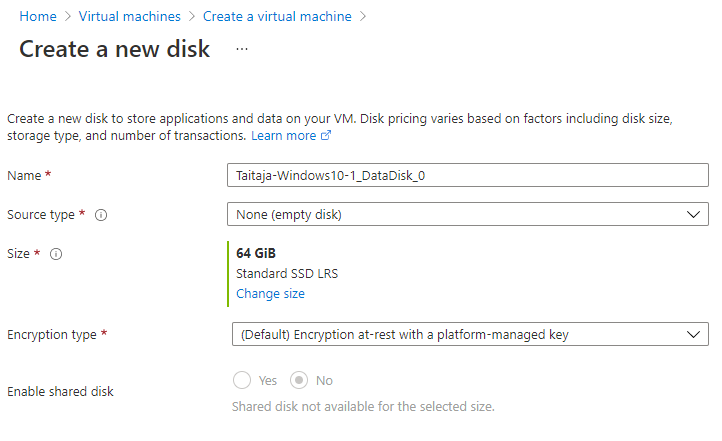
Siirry määrittämään levyn asetuksia seuraavaksi.



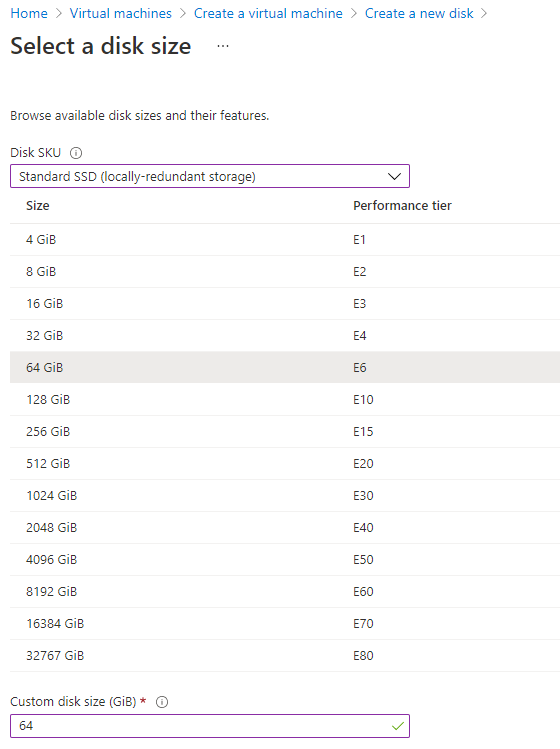
Tässä valitaan, millaisen virtuaalikoneen haluat eli periaatteessa kuinka tehokkaan. Näet listasta mitä ominaisuuksia valitulla koneella on sekä oikealta puolelta sen hinnan kuukaudessa. Mitä tehokkaampi sitä kalliimpi.



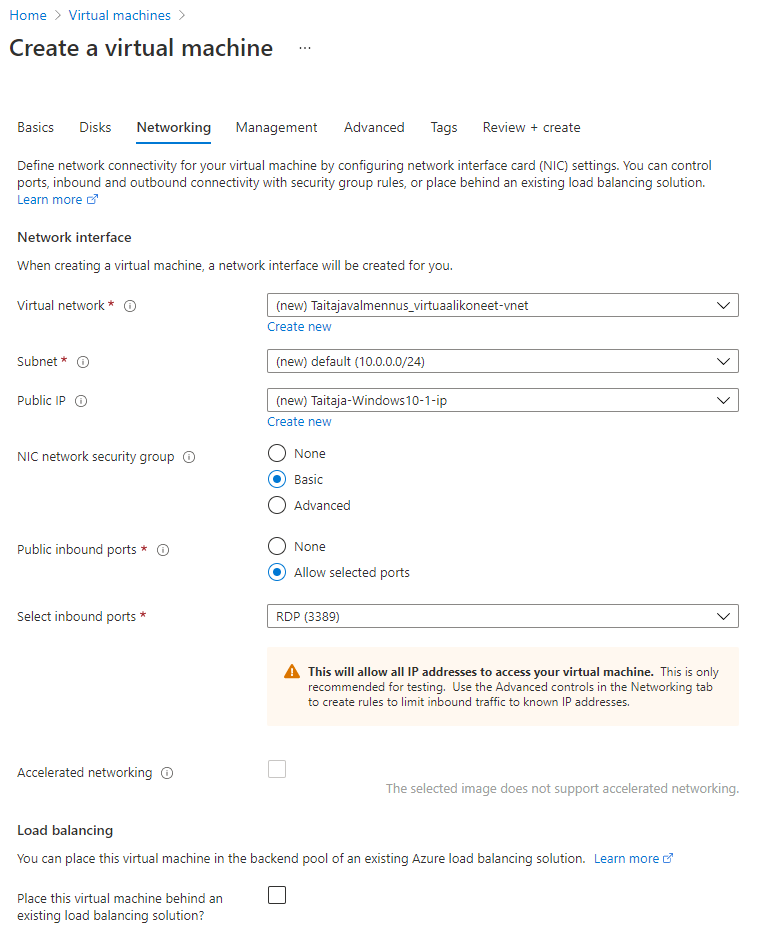
Tässä määritetään, millainen virtuaalikiintolevy virtuaalikoneelle tehdään. Voit valita kiintolevyn ja SSD:n väliltä sekä levyn salaamisen.



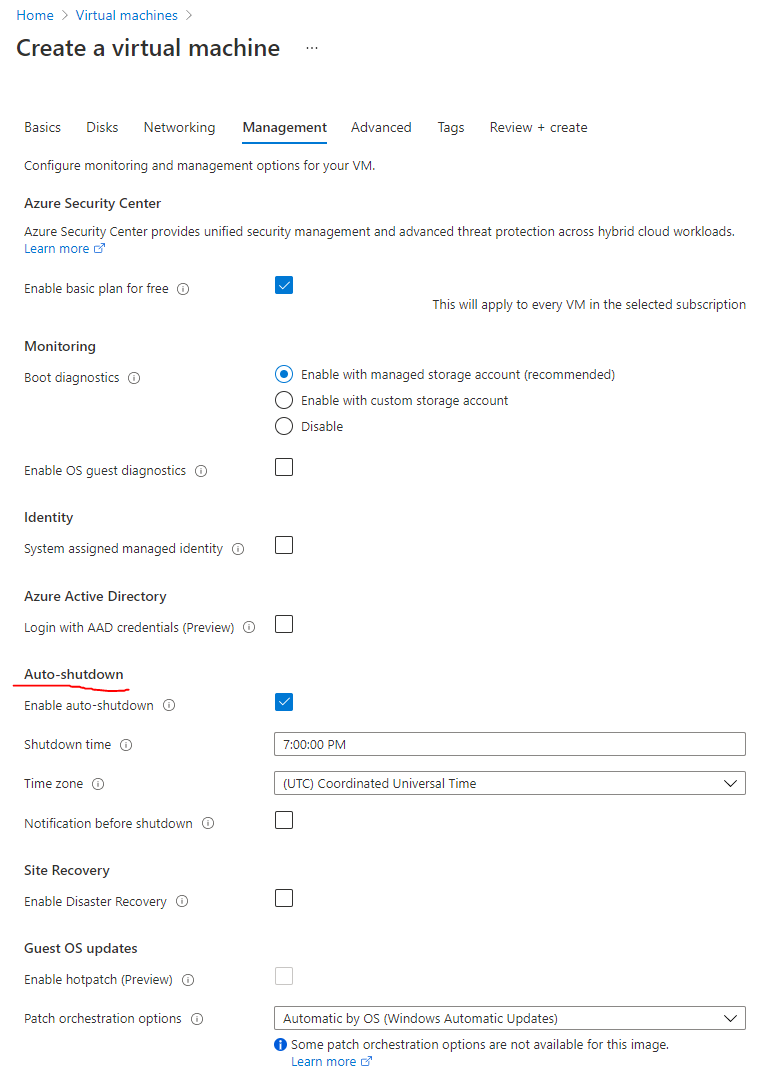
Change size kautta voit tarkemmin valita virtuaalilevyn ja määrittää sen koon.



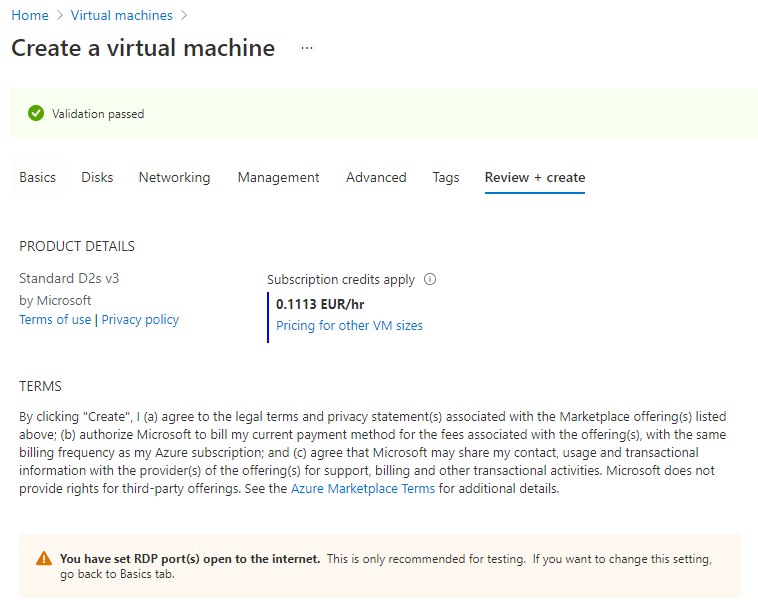
Seuraavaksi määritetään virtuaaliverkon asetukset. Jos tämä on ensimmäinen virtuaalikoneesi, joudut myös luomaan uuden virtuaaliverkon, aliverkon ja julkisen IP-osoitteen.



Sitten virtuaalikoneella määritetään muutamia hallintaan liittyviä asetuksia. Tässä on otettu käyttöön Auto-shutdown, jotta virtuaalikone ei jää päälle kerryttämään kuluja.



Lopuksi hyväksy virtuaalikoneen asetukset. Näet myös arvion sen hinnasta.

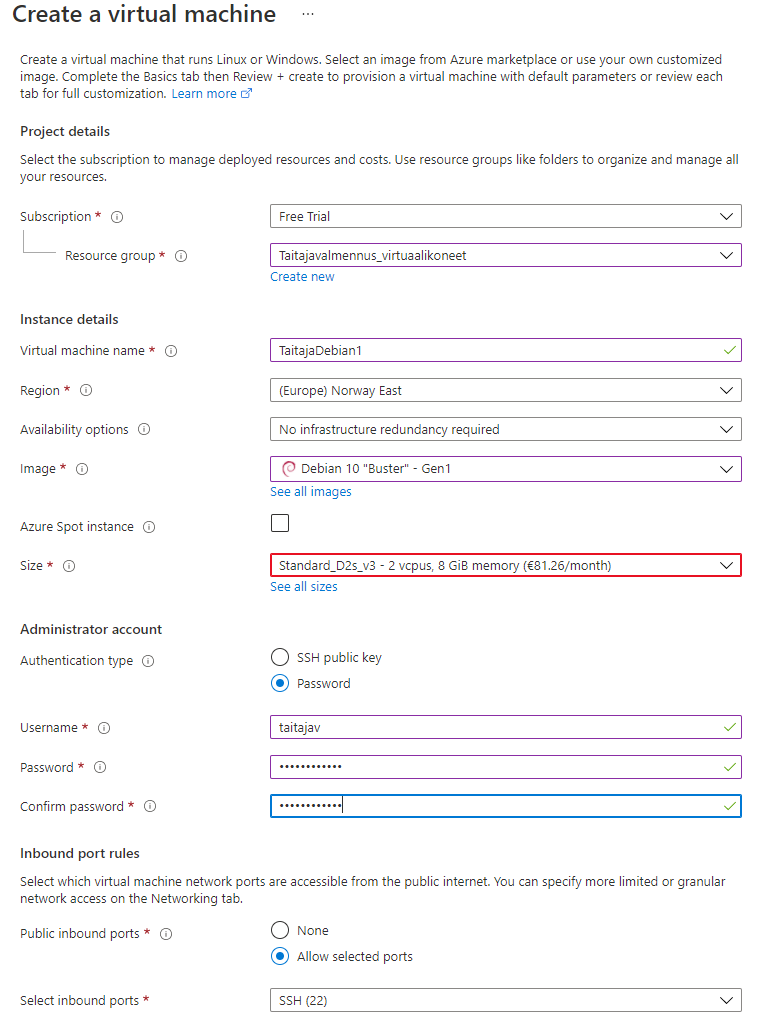


Alhaalta löyty Create painike, joka aloittaa virtuaalikoneen luomisen.



## Linux

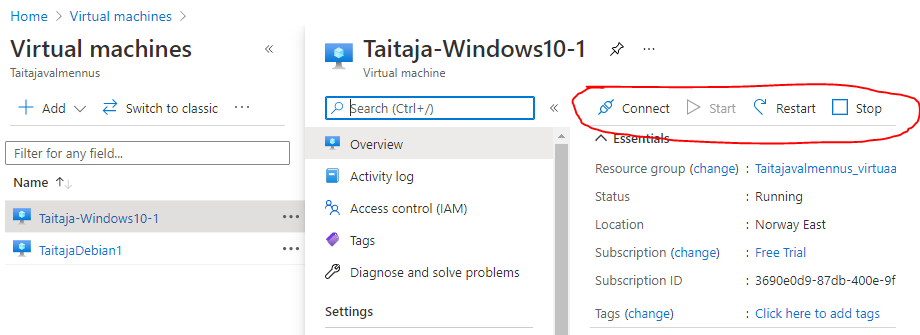
Aloita uuden virtuaalikoneen luominen. Muuten asetukset ovat pitkälti samoja, mutta Image-kohtaan valitaan jokin Linux-distro, kuten tässä Debian. Lopussa valitaan SSH etäyhteyksiä varten.

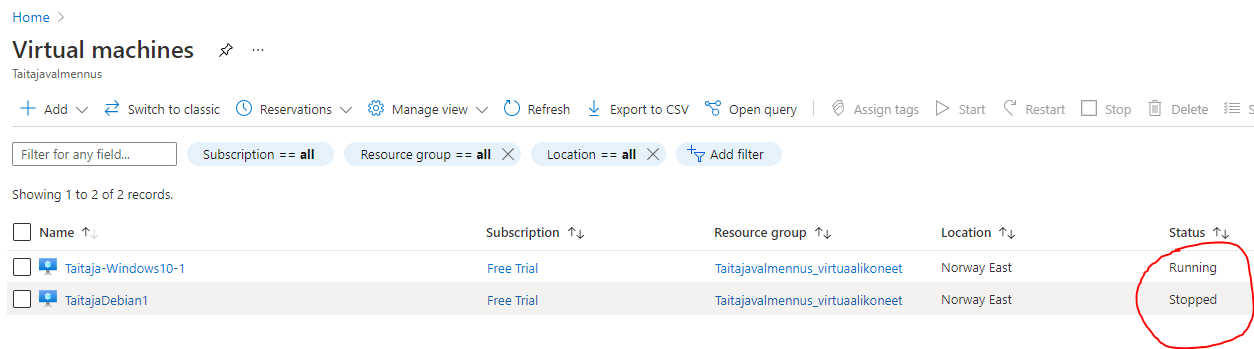


Yhteenvedon jälkeen virtuaalikonetta aletaan luomaan Azureen.

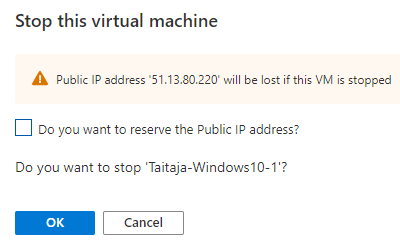


Virtuaalikoneen avaamalla Azuresta saat siitä lisätietoja. Overview valikosta löydät mm. Connect nappulan, jolla saat lisätietoja, miten virtuaalikoneeseen saa yhteyden. Voit myös käynnistää ja sammuttaa virtuaalikoneen.



Virtuaalikoneiden yleisnäkymästä näet, mitkä virtuaalikoneet ovat päällä ja mitkä eivät.

Jos sammutat virtuaalikoneen, saat seuraavanlaisen ilmoituksen.



## Hardened VMs

Azuren Marketplacesta löytyy valmiiksi iso kasa erilaisia virtuaalikoneiden kuvia (imageja). Sieltä löytyy myös valmiiksi kovennettuja virtuaalikoneita, eli niissä on valmiiksi paljon tietoturvallisia asetuksia tehtynä. Löydät näitä Marketplacesta helposti hakusanalla ”CIS”.

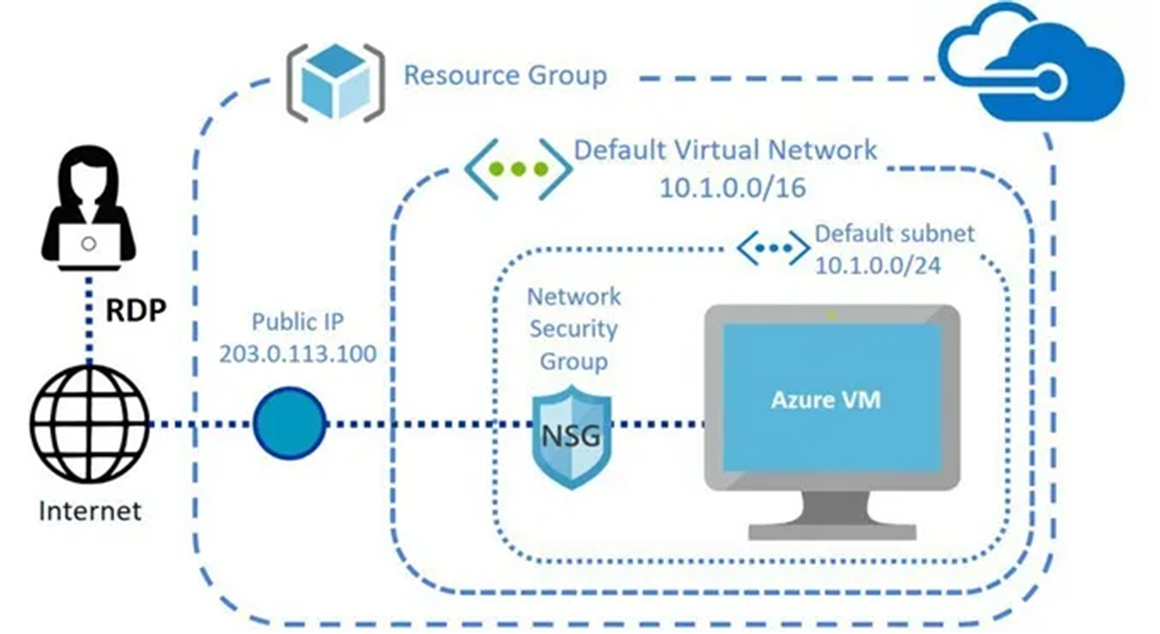
## Lisäosat (Extension)

Kuten selaimiin, myös Azuren virtuaalikoneisiin voi lisätä lisäosia. Näillä saadaan erilaisia lisätoimintoja lisätyksi virtuaalikoneelle.

# Virtuaaliverkot

Azuresta löytyy paljon verkkoihin liittyviä asetuksia. Tärkeintä on hahmottaa, että ensin tulee virtuaaliverkko ja sen sisällä on aliverkko tai useita aliverkkoja. Aliverkkojen tulee olla virtuaaliverkon osoitealueella. Tyypillisesti näillä verkoilla on myös yksi julkinen IP-osoite, jotta niihin tai niiden laitteisiin voidaan muodostaa yhteys internetistä.

Alla olevassa kuvassa käyttäjä muodostaa etäyhteyden RDP-ohjelmalla internetin kautta julkiseen IP-osoitteeseen 203.0.113.100. Azuren puolella on käytössä yksityinen verkko 10.1.0.0/16 ja sen sisältä aliverkko 10.1.0.0/24. Tämän aliverkon sisällä on vielä palomuuri eli NSG, joka suodattaa yhteyksiä ennen kuin yhteys saapuu Azure VM virtuaalikoneelle.



Alla olevassa kuvassa virtuaaliverkosta löytyy 2 verkkokorttia ja AzureBastion.

A screenshot of a computer

Description automatically generated

Virtuaaliverkon osoitealue on 10.0.0.0/16 eli todella paljon osoitteita.

Graphical user interface

Description automatically generated with medium confidence

Tässä tarkempia tietoja verkkokortista, joka on kytketty Windows 10 virtuaalikoneeseen.

Graphical user interface, text, application, email

Description automatically generated

## Network Security Groups (NSG)

NSG:t ovat ikään kuin palomuureja, joilla voidaan tehdä sääntöjä verkoille ja virtuaalikoneille.

Graphical user interface, text, application, email

Description automatically generated

Tässä Windows 10 koneen säännöt, jossa mm. sallitaan RDP yhteys virtuaalikoneelle. Priority kohdalla määritetään, missä järjestyksessä säännöt käydään läpi, pienimmästä suurimpaan.

Tänne voisi tehdä myös sääntöjä, jos halutaan esimerkiksi sallia yhteydet FTP, WWW tai muuhun palveluun.

A screenshot of a computer

Description automatically generated

Esimerkiksi tässä sallitaan sisääntuleva http-yhteys (www-sivut) tälle virtuaalikoneelle.

Graphical user interface, application

Description automatically generated

NSG avulla voisit myös sallia etäyhteydet vain tietyistä IP-osoitteista esimerkiksi virtuaalikoneille. Tällöin yllä olevassa kuvassa tulisi muokata myös Source kohtaa, johon voisi laittaa sitten halutut IP-osoitteet.

## Diagram

Virtuaaliverkon rakenteen näet Diagram valikon kautta.

Graphical user interface, application

Description automatically generated with medium confidence

# Yhteys virtuaalikoneeseen

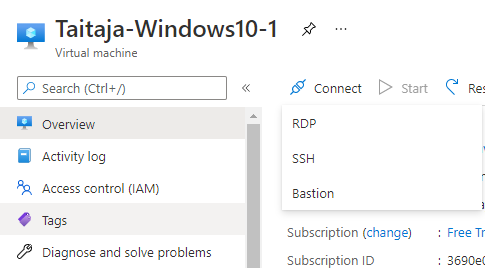
Yhteyden muodostaminen virtuaalikoneeseen riippuu sen käyttöjärjestelmistä ja Azuren asetuksista. Tässä käydään usea eri tapa läpi.

## RDP

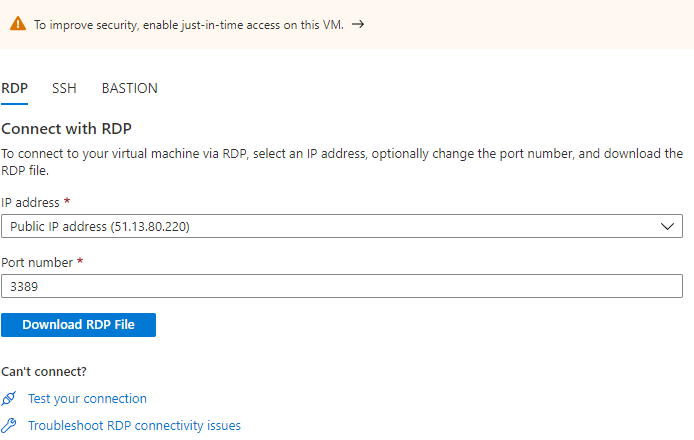
Windows virtuaalikoneeseen saat muodostettua helposti yhteyden RDP eli Remote Desktop Connection työkalulla. Avaa virtuaalikoneen asetukset.



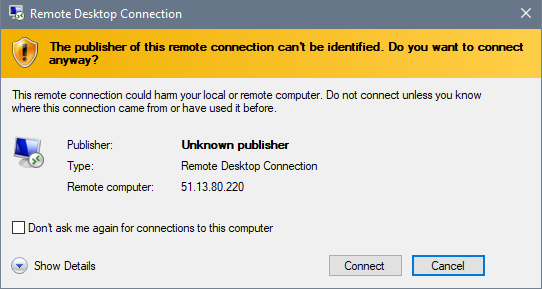
Connect kohdasta valitse RDP.



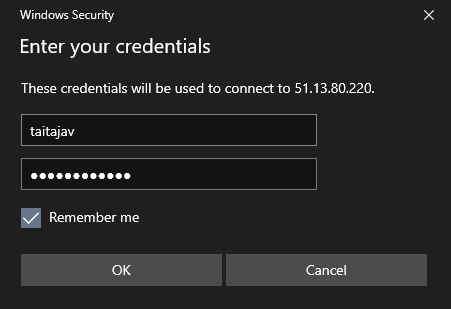
Näkymässä kerrotaan virtuaalikoneen julkinen IP-osoite sekä portti. Download RDP file saat ladattua RDP-tiedoston koneellesi, jolla voit helposti muodostaa etäyhteyden virtuaalikoneeseen.



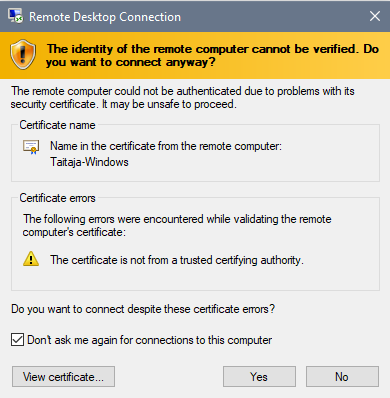
RDP toimii aivan normaalisti, kuten olet aikaisemminkin opinnoissasi käyttänyt.



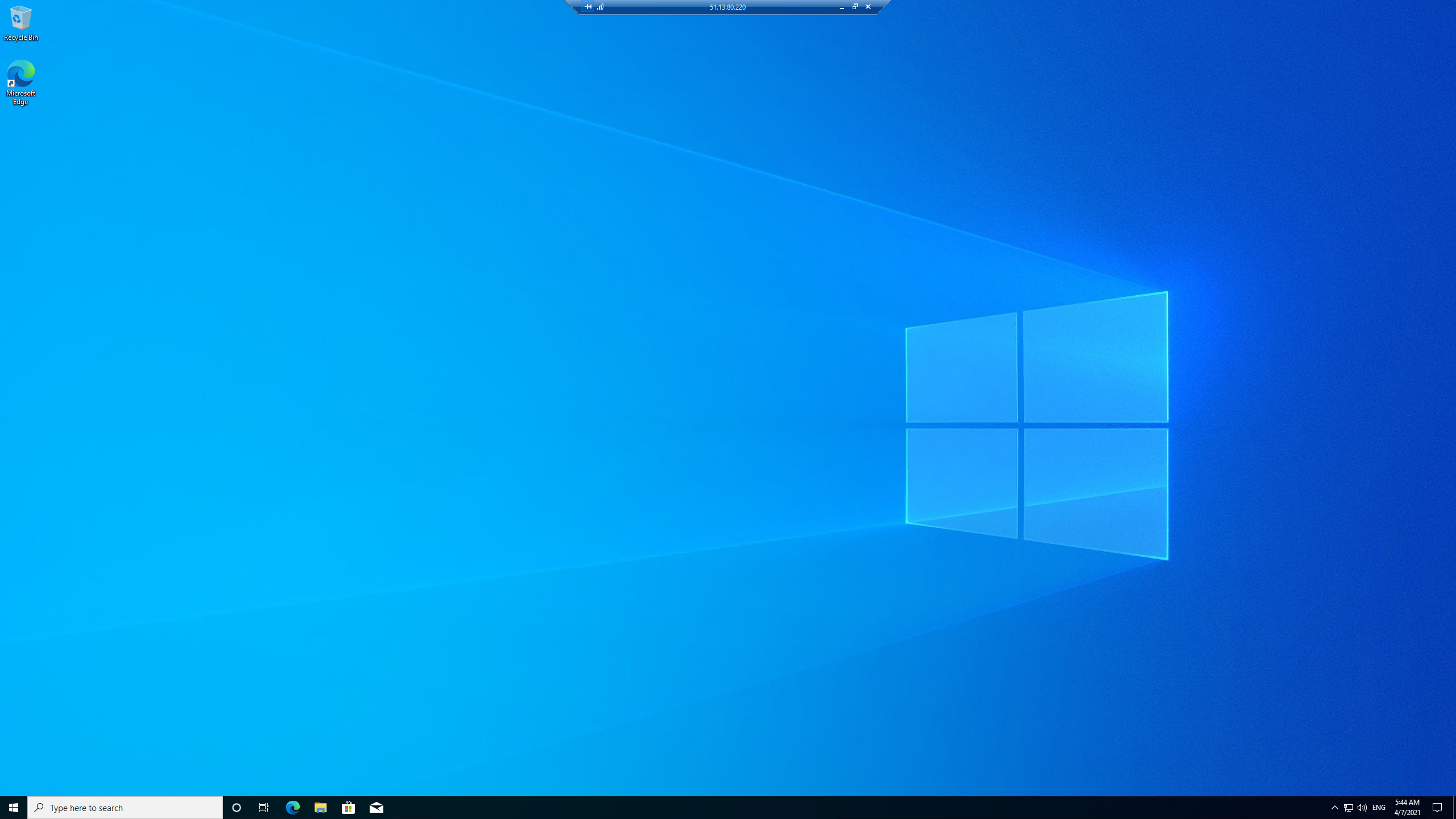
Anna tunnukset, jotka määritettiin virtuaalikonetta luodessa.



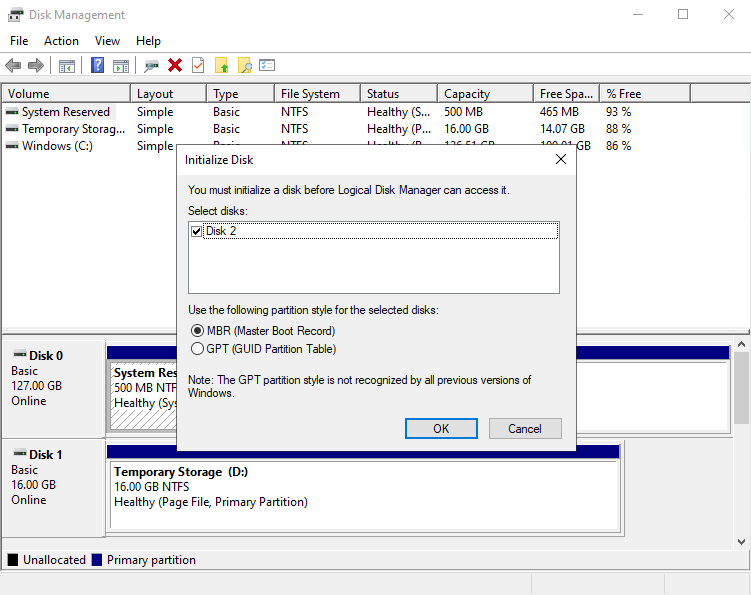
Hyväksy sertifikaatti.



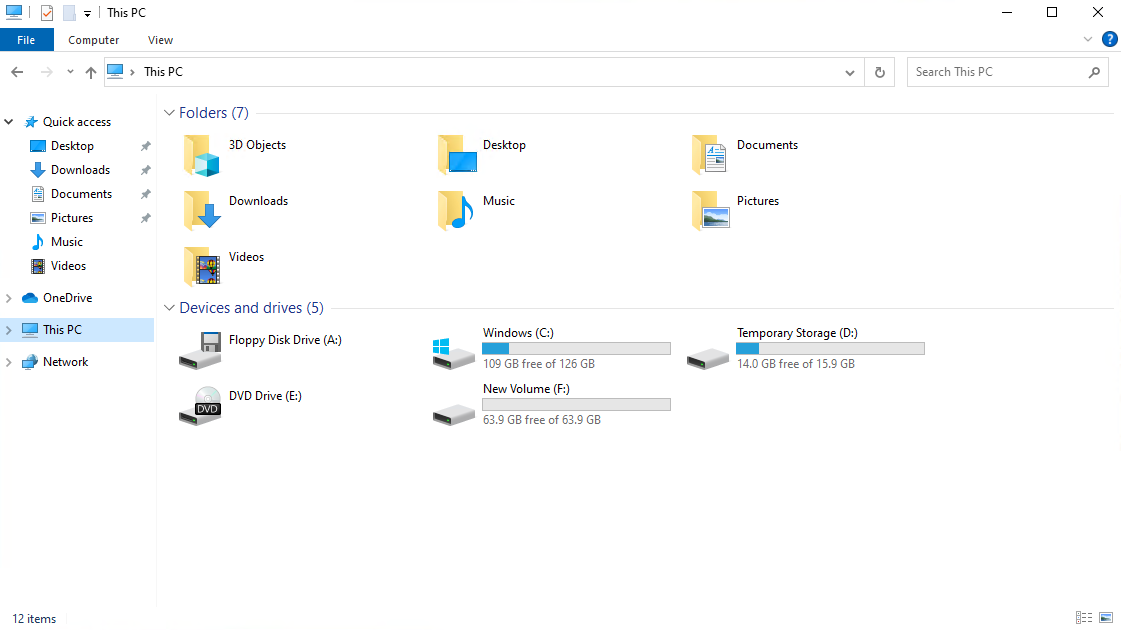
Etäyhteys RDP:llä on nyt muodostettu virtuaalikoneeseen.



Koska tälle virtuaalikoneelle lisättiin toinen kiintolevy sitä luodessa, se tulee ottaa käyttöön Disk management kautta.

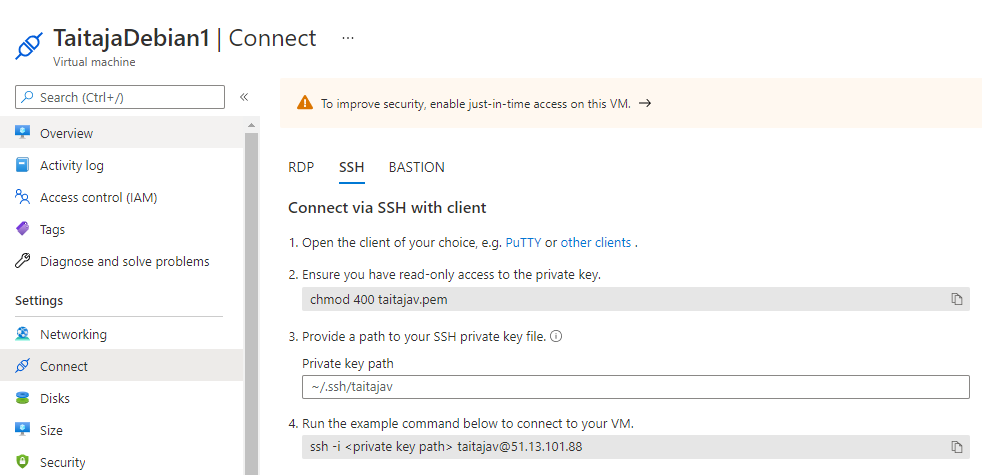


Toinen levy toimii ja löytyy File Explorerin kautta.

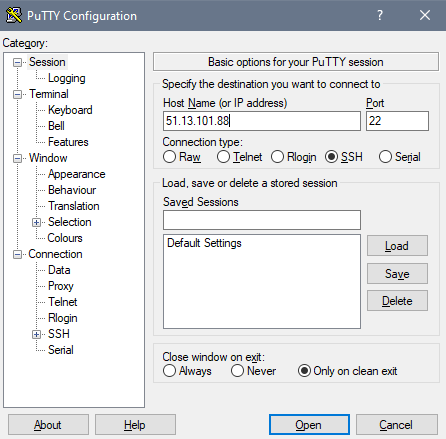


## SSH

Linux koneeseen SSH-yhteys. Mene virtuaalikoneen asetuksiin ja Connect valikon kautta pääset SSH-asetuksiin. 4 kohdasta näet IP-osoitteen, johon voit muodostaa esimerkiksi Putty-ohjelmalla yhteyden.

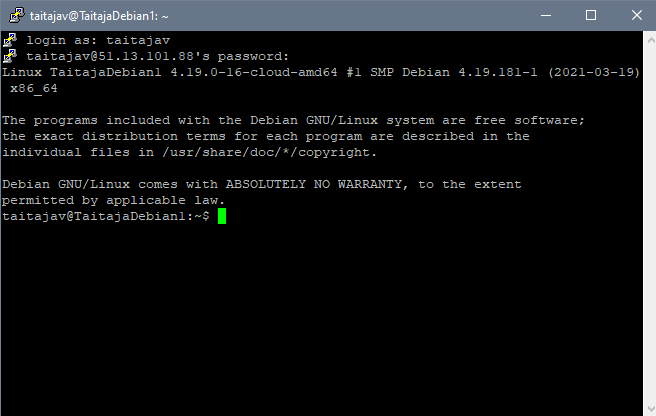


SSH-yhteys Puttylla.

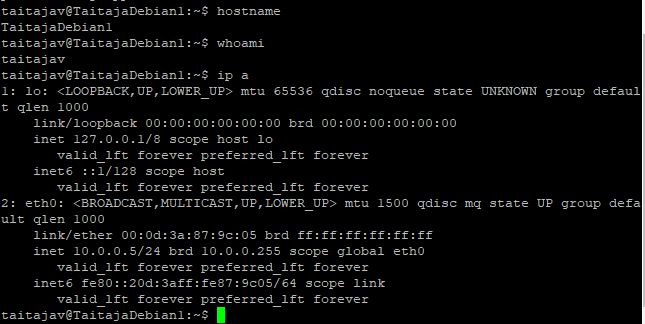


Yhteys muodostettu virtuaalikoneeseen. Ennen tätä saatat joutua hyväksymään sertifikaatin.

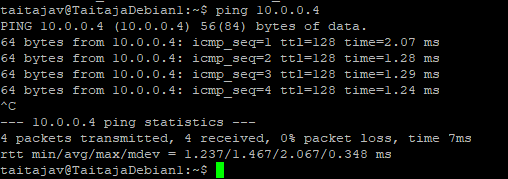
**Vinkki: Putty on siitä kätevä, että voit helposti kopioida siihen tekstiä ja komentoja esimerkiksi netistä löytyvistä ohjeista. Ei tarvitse siis aina kirjoittaa pitkiä komentoja!**



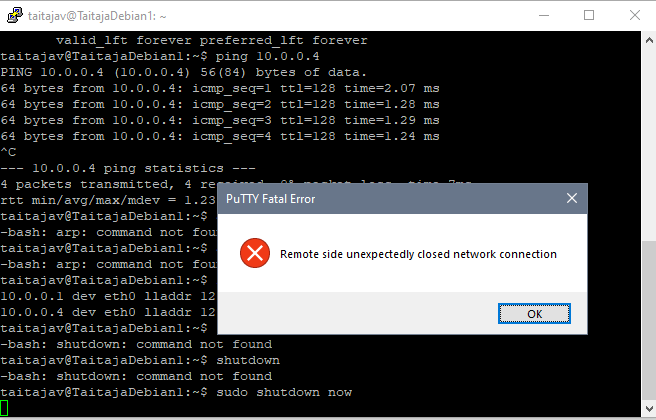
Testataan, että kaikki pelittää.



Pingataan Windows 10 virtuaalikoneen IP-osoitetta.



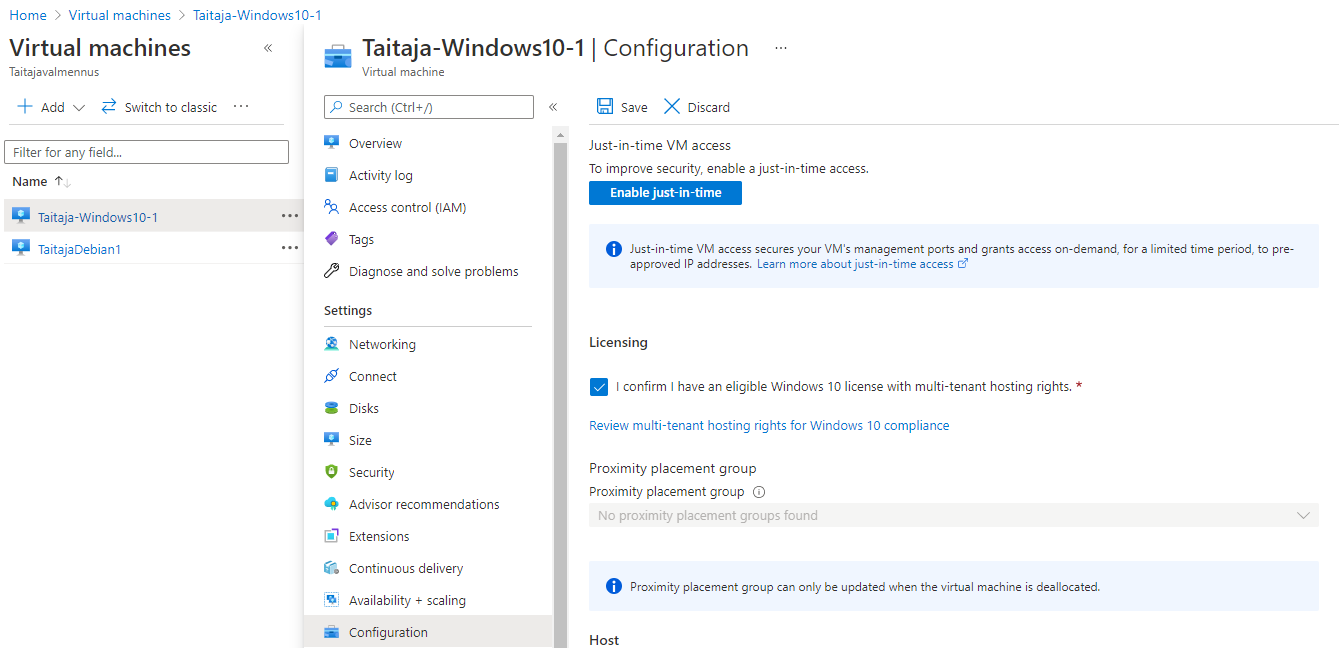
Sammutetaan virtuaalikone.



## Just-in-time (JIT)

Virtuaalikoneita ei saisi jättää ”avoimeksi” pilveen, koska silloin kuka tahansa voisi yrittää muodostaa niihin RDP/SSH yhteyden kokeilemalla tarpeeksi pitkään. Virtuaalikone halutaan pitää kuitenkin päällä, mutta jotta siihen saa muodostettua etäyhteyden, tulee siihen anoa lupaa Azuren kautta. Tällöin kuka tahansa ei voi muodostaa etäyhteyttä.

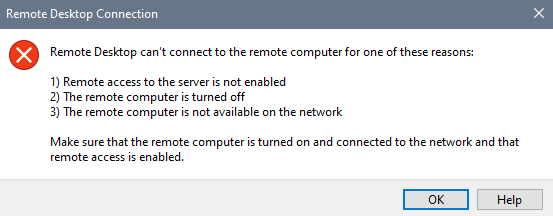
Tässä luodaan JIT-käytäntö Windows 10 virtuaalikoneelle.



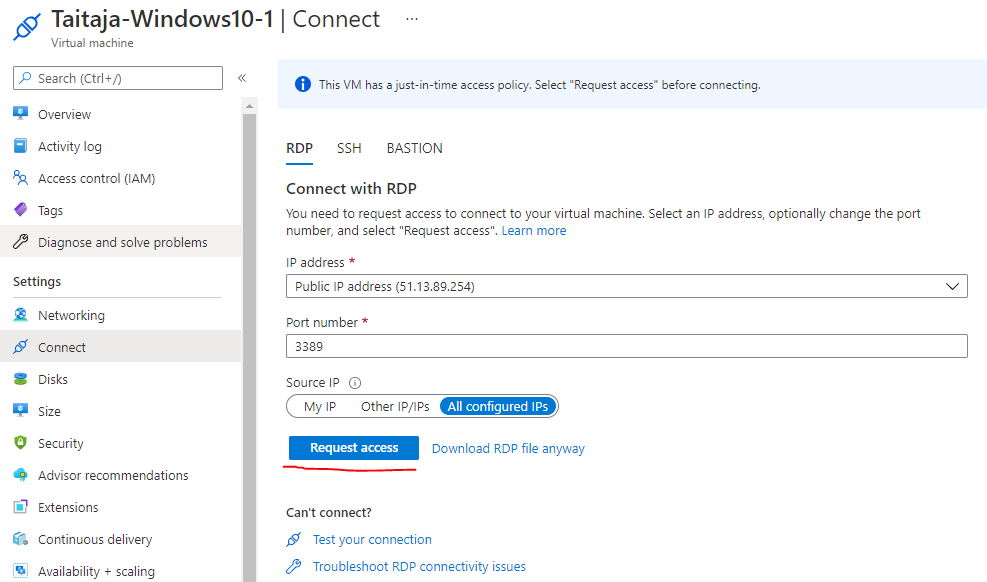
JIT on nyt otettu käyttöön.



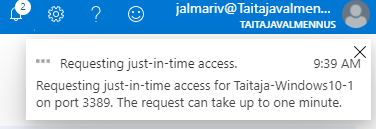
Testataan voiko RDP:llä muodostaa etäyhteyden virtuaalikoneeseen. Ei onnistu, koska lupaa ei ole anottu.



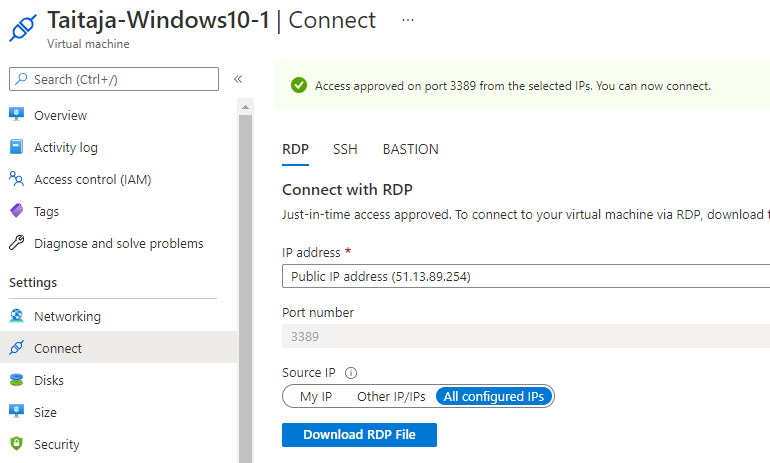
Mene Windows 10 koneen asetuksiin ja Connect kohtaan. Kuvan mukaisesti sieltä voit anoa lupaa etäyhteyttä varten.



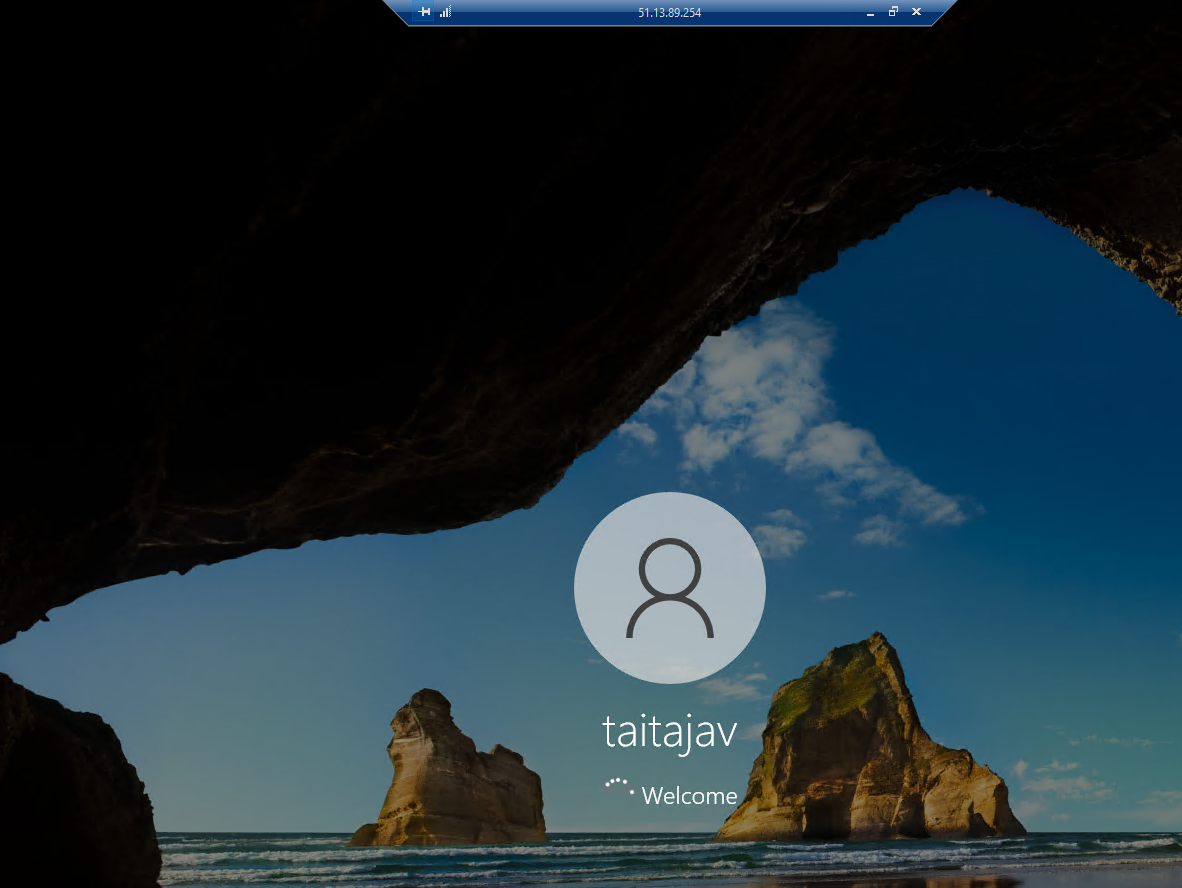
Anomisessa kestää hetken aikaa.



Hetken päästä voit ladata RDP tiedoston.

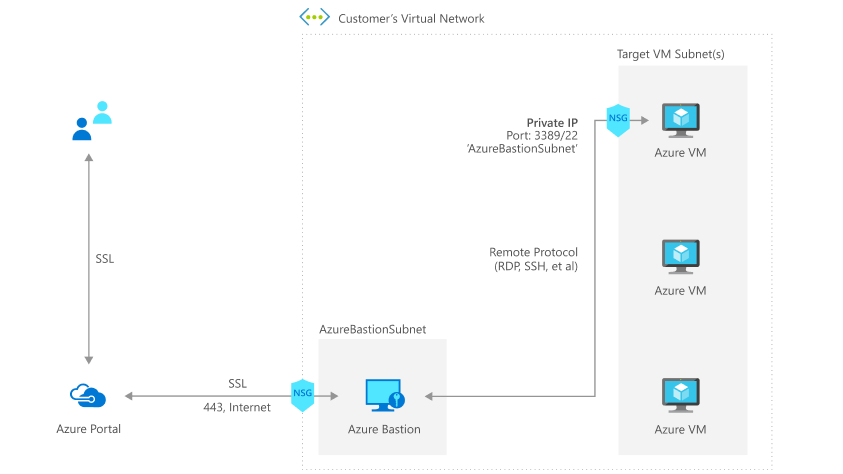


Ja muodostaa etäyhteyden.

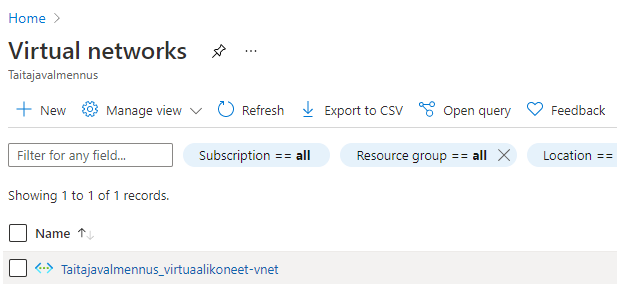


## Bastion

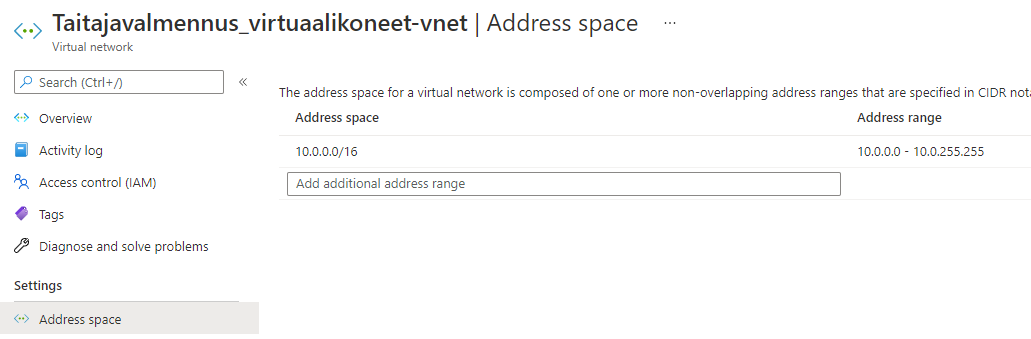
Bastionin ideana toimia ikään kuin välityspalvelimena Azure Portaalin ja virtuaalikoneiden välillä. Sen avulla voit muodostaa etäyhteyden virtuaalikoneisiin myös selaimen kautta.



Mene Azuren virtuaaliverkkoihin. Siellä tulisi olla ainakin yksi verkko, joka luotiin samalla, kun luotiin virtuaalikoneita.

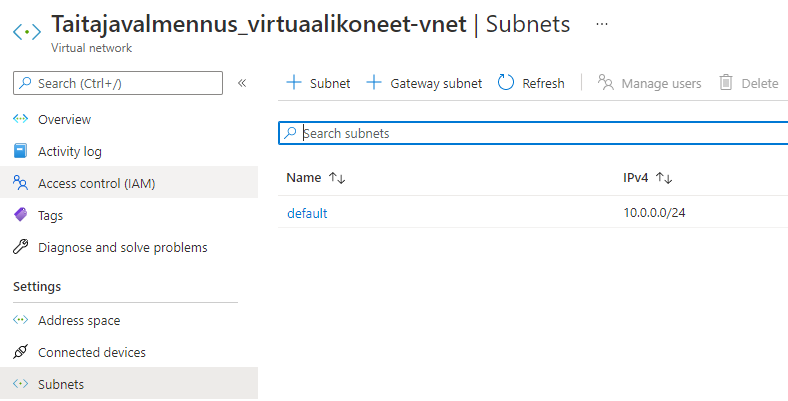


Tässä osoitealuetta muutettiin 10.0.0.0/16, kun se aikaisemmin oli 10.0.0.0/24, jotta saatiin enemmän osoitteita käyttöön Bastionia varten.

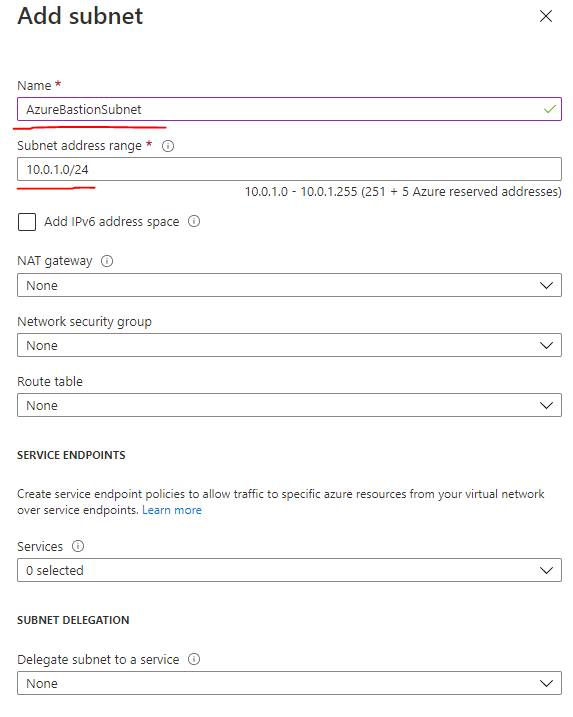


Seuraavaksi luodaan uusi aliverkko virtuaaliverkon sisälle.

Oletusverkko löytyy jo, luodaan uusi.



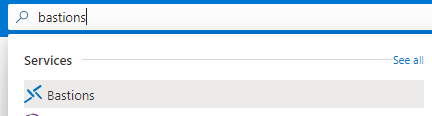
Bastionille tarkoitetun aliverkon nimeksi on PAKKO laittaa AzureBastionSubnet, kuten kuvassa on tehty, muuten se ei toimi. Sen osoitealueeksi määritetään 10.0.1.0/24 (default verkon on 10.0.0.0/24), jotta niiden osoitealueet ovat eri.



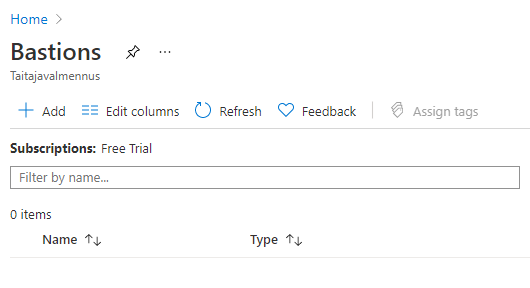
Nyt virtuaaliverkossa on kaksi aliverkkoa, default virtuaalikoneille ja AzureBastionSubnet Bastion-palvelulle.



Seuraavaksi tulee luoda itse Bastion. Käytä Azure portalin hakua.

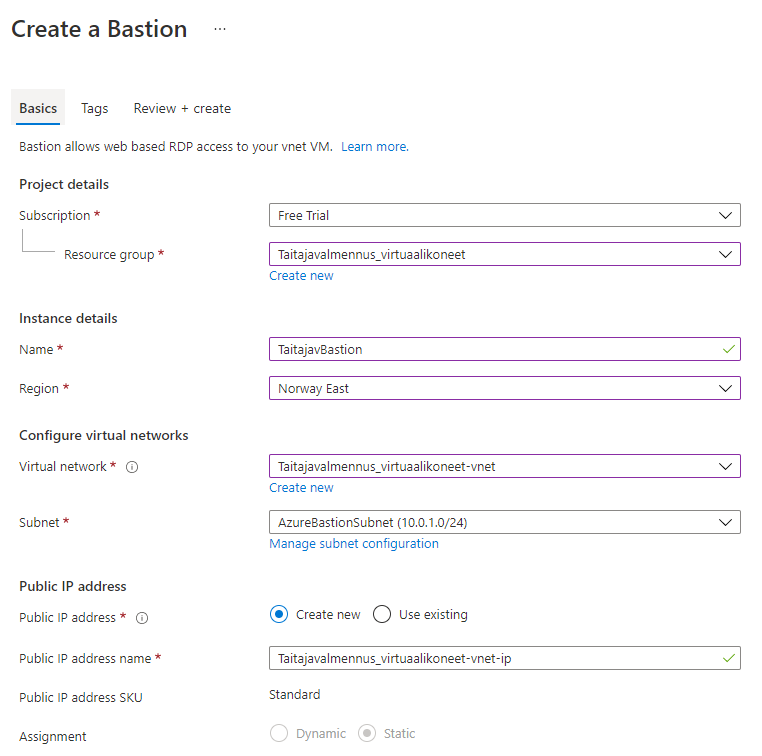


Bastions kautta luo uusi Bastion.

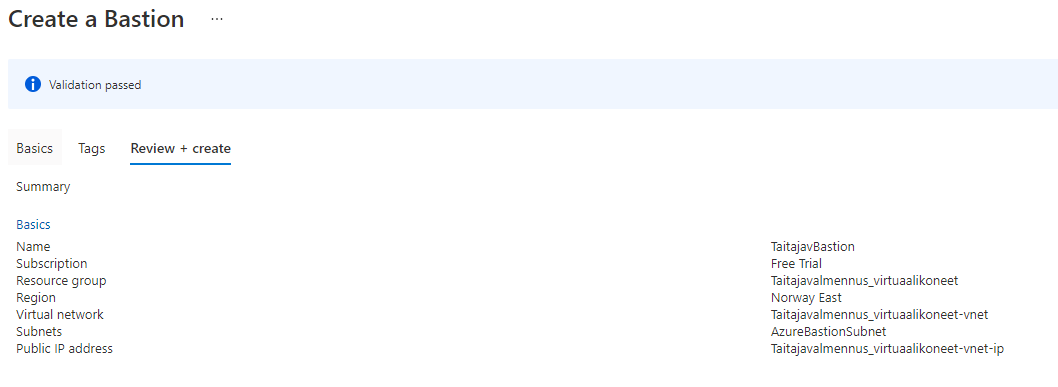


**Tässä on tärkeätä, että Region on sama, kuin jossa virtuaaliverkot ja aliverkotkin ovat!**

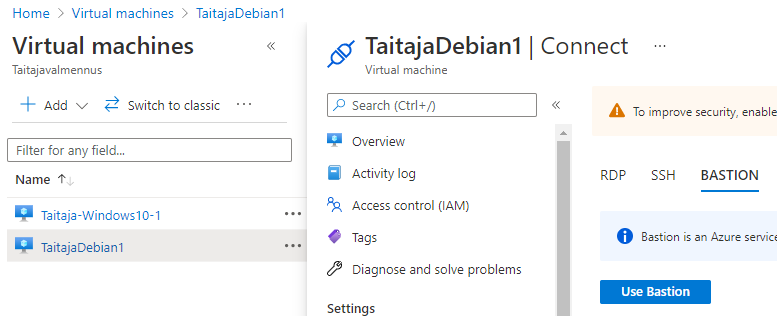
Anna nimi. Valitse virtuaaliverkko sekä aliverkko (AzureBastionSubnet). Jos näitä ei löydy ehdotuksista, tarkista että Region on varmasti oikein.



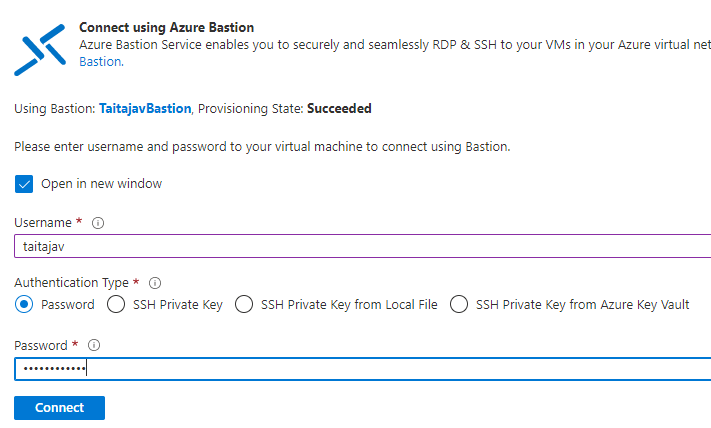
Luo Bastion.



Bastionin luomisen jälkeen mene virtuaalikoneen asetuksiin. Paina Use Bastion.

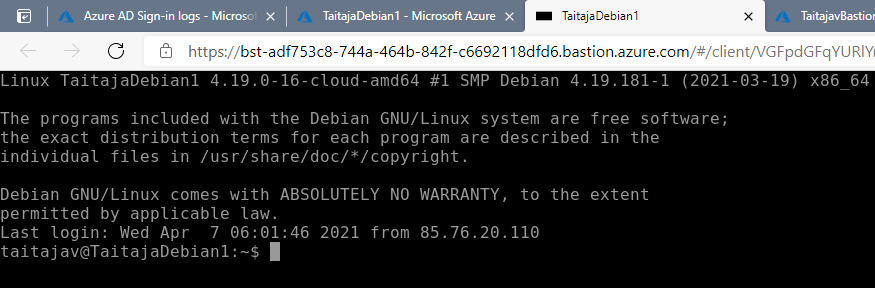


Uudesta näkymästä voit valita avataanko etäyhteys uuteen välilehteen vai nykyiseen. Anna virtuaalikoneen käyttäjätunnus ja salasana (tai avain).



Tässä vaiheessa selain saattaa estää Pop-upin aukeamasta, muokkaa selaimesi asetuksia tarvittaessa, jotta ne on sallittu. **Muista laittaa virtuaalikone päälle, jotta Bastionin kautta siihen saa etäyhteyden!**

Tässä etäyhteys avautui toiseen välilehteen. Bastionista löytyy myös leikepöytä, eli voit esimerkiksi kopioida komentoja virtuaalikoneelle.



## Virtuaalikiintolevyjen salaaminen

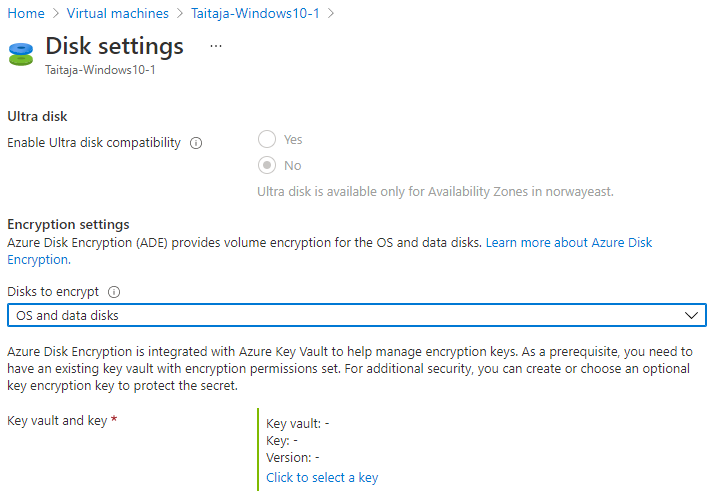
**Jos tämän kanssa tulee ongelmia lue tämä läpi ja anna Resource Groupille oikeuksia eli anna Key Vault Reader oikeudet itsellesi:**

<https://docs.microsoft.com/en-us/answers/questions/570921/getting-34caller-needs-data-action34-while-enablin.html>

Virtuaalikoneen tulee olla päällä, jotta voit salata sen levyn. Tässä salataan Windows 10 -virtuaalikoneen levy. Valitse Additional settings.

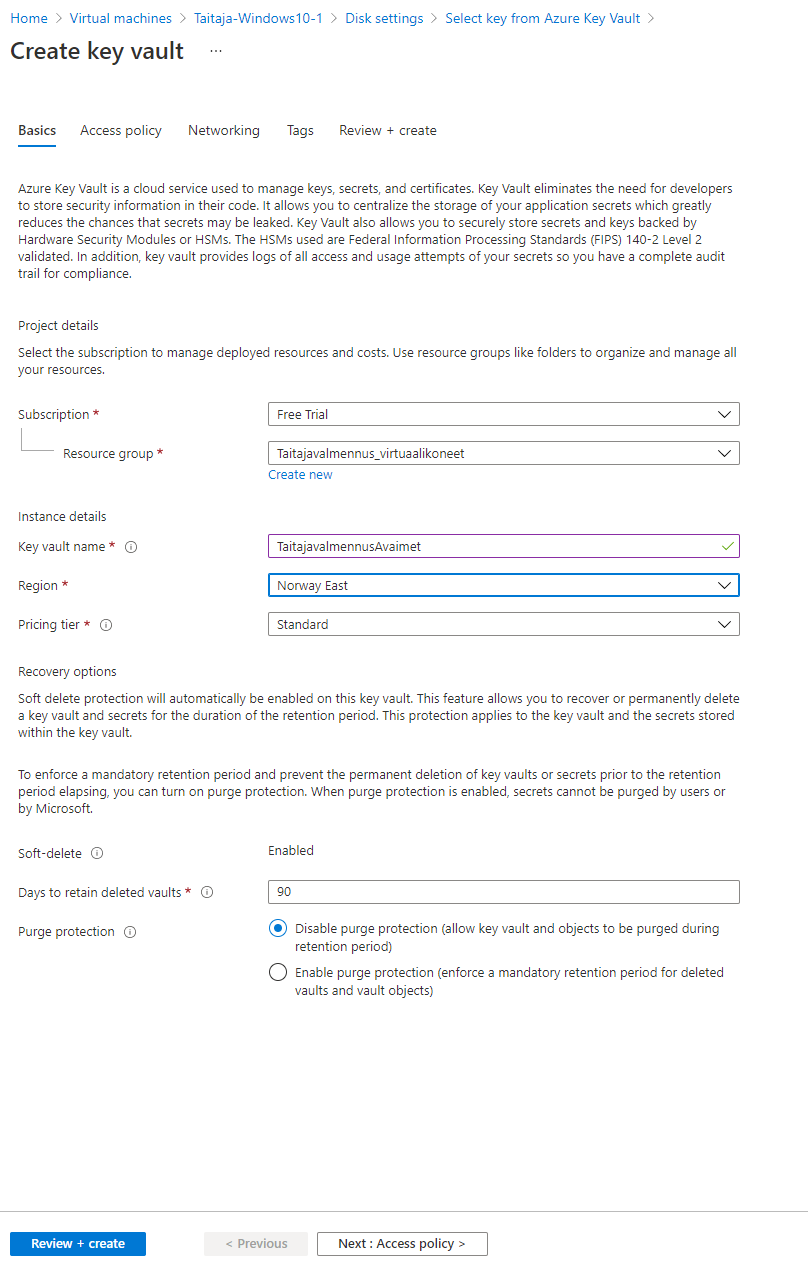


Salataan käyttöjärjestelmä ja data levyt. Joudut luomaan myös uuden avainsäilön (Key vault) sekä avaimen sinne kohdan Click to select a key kautta.

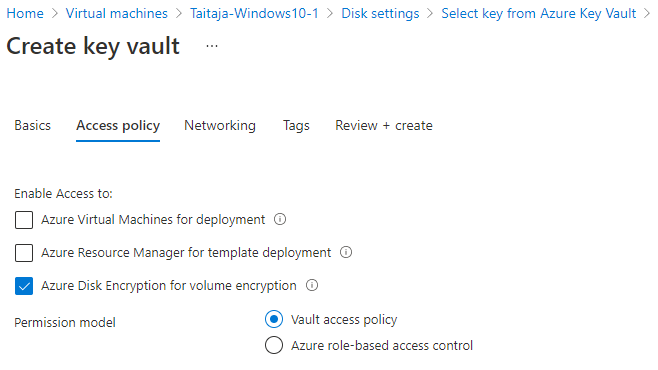


Tässä luodaan uusi avainsäilö.

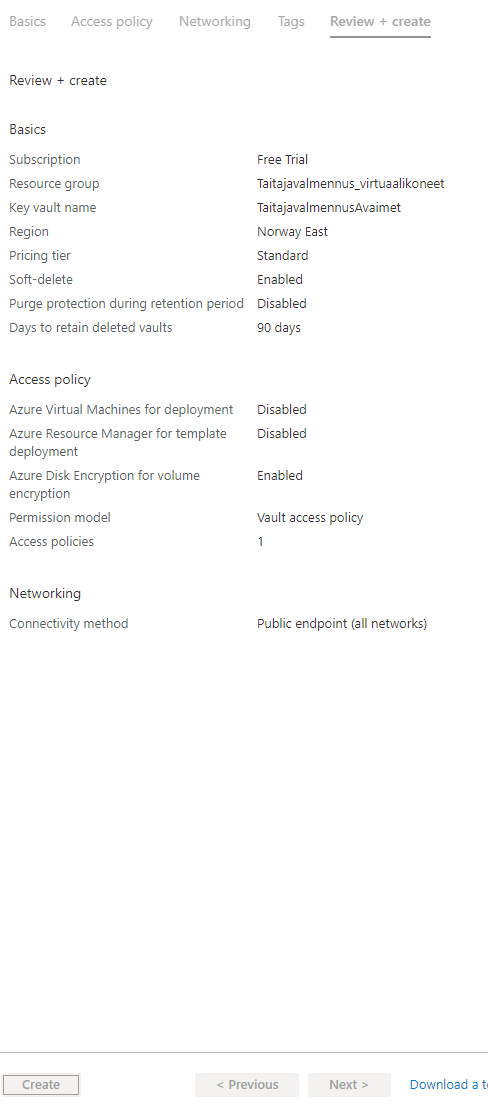
**Huomioi, että avainsäilön tulee olla samassa Regionissa kuin virtuaalikonekin!**



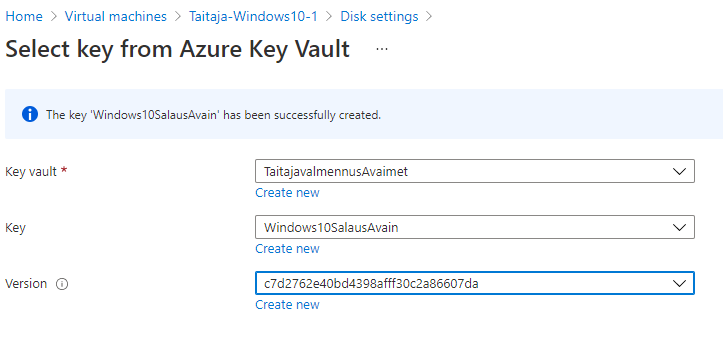
Määritetään, että näillä avaimilla voidaan salata levyjä.



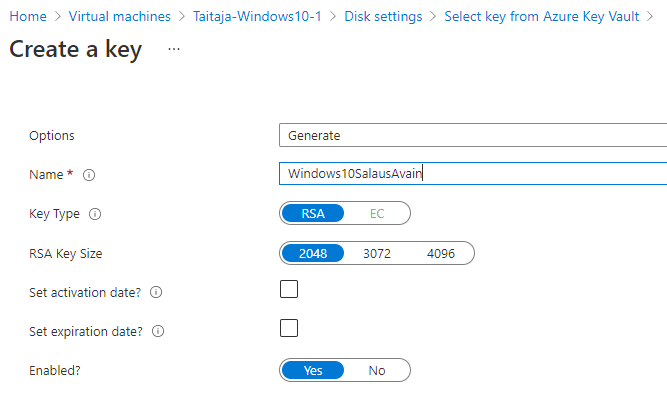
Hyväksytään yhteenveto.



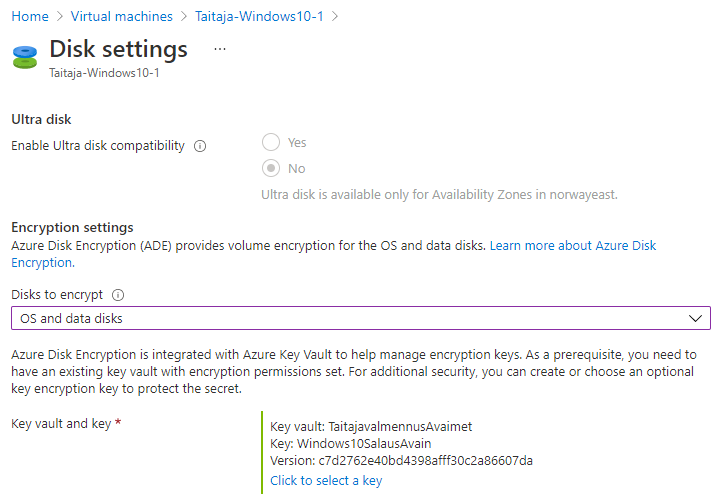
Avainsäilön luomisen jälkeen sinut ohjataan luomaan itse avainta. Luo uusi avain Key kohdassa.



Määritä avaimelle tarkemmat tiedot. Muista ottaa se käyttöön Enabled? kohdasta.



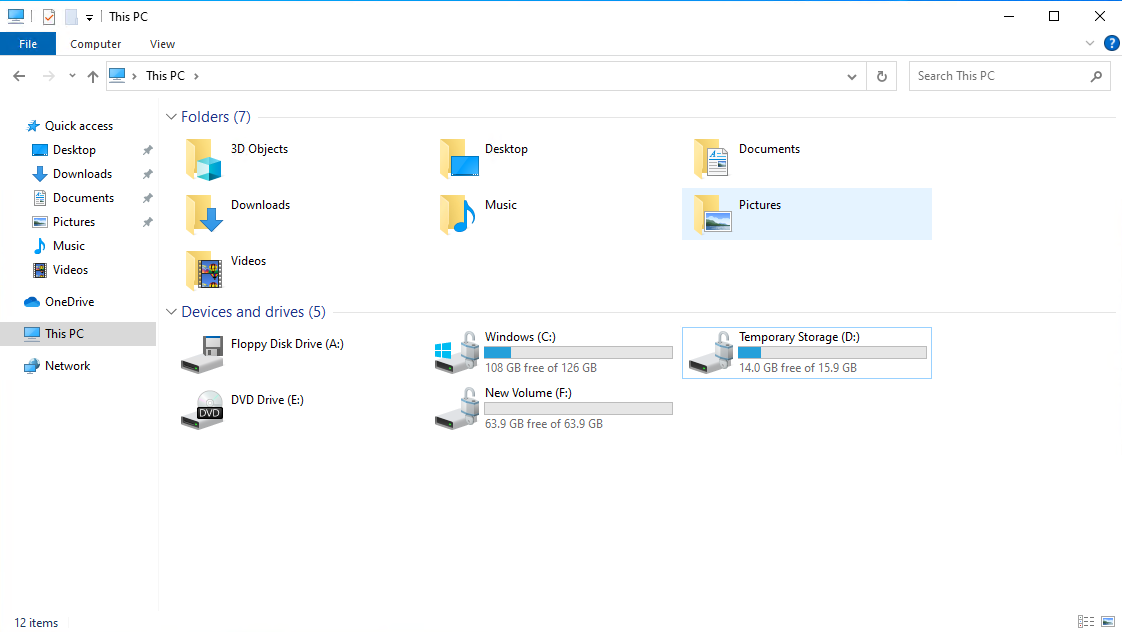
Pääset takaisin levyn salaamiseen. Kuvasta käy ilmi, että salaamiseen käytetään avainta Windows10SalausAvain, joka löytyy avainsäilöstä TaitajavalmennusAvaimet. Tallenna asetukset.



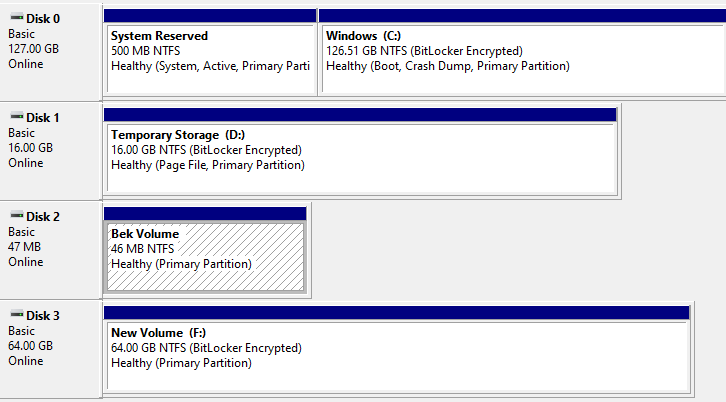
Virtuaalikoneen asetuksista näet, että molemmat koneen levyt on salattu.



Kirjautumalla virtuaalikoneelle näet, että kiintolevyjen ikonissa on lukon kuva.



Samoin Disk Managementin kautta näet, että levyt on salattu Bitlockerilla.



Myös Linux virtuaalikoneiden kiintolevyjä on mahdollista salata.