Lauri Partinen(ktkt23sp)

CARP
Juustomarket

Tietoturvalaitteet

2025

Kaakkois-Suomen
ammattikorkeakoulu

SISÄLLYS

1 JOHDANTO

Common Address Redundancy Protocol (CARP) on verkkoprotokolla, joka on suunniteltu tarjoamaan käytettävyyttä ja kuormituksen kontrollointia ip-osoitetasolla eri yrityksille. Protokollan sisällä useat samassa verkkosegmentissä olevat hostit voivat tehokkaasti jakaa yhden IP-osoitteen, jolloin yksi toimii isäntänä ja muut käyttäjät varalla. Pääisännän poisjäämisessä tai palvelun vikatilanteessa yksi varaisännistä ottaa haltuunsa jaetun IP-osoitteen, jolloin palvelun jatkuva saatavuus ja minimaaliset toiminnan häiriöt ovat mahdollista. Carp kehitettiin alkujaan ilmaisen ja avoimen lähdekoodin vaihtoehtona patentoidulle Virtual Router Redundancy Protocol (VRRP). Palvelu tarjosi yrityksille kustannustehokkaan ratkaisun verkon redundanssin toteuttamiseen koko yrityksen toimintaympäristössä.

1.1 Miten Carp toimii

Carp toimii mahdollistamalla ryhmälle isäntäkoneita jakamaan vastuun virtuaalisesta IP-osoitteesta. Hostit muodostavat redundanssiryhmän tai Carp-ryhmän. Ryhmässä yksi isäntäkone on nimetty isännäksi, joka vastaa aktiivisesti kaikkiin jaettuun IP-osoitteeseen lähetettyihin pyyntöihin. Muut isännät pysyvät valmiustilassa valvoen jatkuvasti isäntäkonetta ja valmiina ottamaan hallinnan järjestelmästä tarvittaessa. Carp:n toimintamekanismi sisältää useiden kriittisten komponenttien yhteistyötä. Jokainen Carp-ryhmän isäntäkone saa prioriteettiarvon konfiguroinnin aikana. Korkeimman prioriteetin omaavasta isännästä tulee automaattisesti isäntäkone, joka ottaa aiemmalta isännältä virtuaalisen IP-osoitteen hallinnan haltuunsa. Ylläpitääkseen tilaansa isäntäkone lähettää säännöllisesti mainosviestejä muille jäsenille ilmoittaakseen aktiivisesti toiminnasta isäntänä. Mainokset toimivat aktiivisuus signaaleina Carp-ryhmässä. Jos varaisännät havaitsevat, että isännän mainosviestit ovat loppuneet ryhmässä päätetyn aikajanan yli. Käynnistetään vikasietoprosessi., jonka aikana varakoneet suorittavat valinnan niille annettujen prioriteettiarvojen perusteella. Korkeimman prioriteetin omaavasta varakoneesta tulee uusi isäntä ja ottaa vastuun virtuaalisen IP-osoitteen hallitsemisesta. Uusi isäntä alkaa käsitellä IP-osoitteeseen suunnattua liikennettä varmistaen palvelun jatkuvuuden ja saatavuuden koko siirtymän ajan.

Carp-kehyksen turvallisuuden parantamiseksi protokolla toteuttaa todennuksen jaetun salassa olevan salasanan avulla. Kaikki Carp-ryhmän isäntien välinen viestintä on todennettava asianmukaisesti jaetulla salasananalla, mikä estää tehokkaasti ulkopuolelta tulevia luvattomia isäntiä liittymästä ryhmään tai lähettämästä vääriä mainoksia, jotka voisivat häiritä Carp-ryhmän toimintaa.

1.2 Juustomarket implementointi

Juustomarket koostuu monesta erilaisesta verkko segmentistä ja sijanneista. Organisaatio ylläpitää verkkosegmenttejä toimistolle ja varastolle, jotka yhdistyvät sisäiset verkot ulkoisiin juustomarketin resursseihin. Carp näkökulmasta juustomarkettiin capr toteutus on mahdollista toteuttaa. Carp tarjoaa laadukkaan kriittisten palveluiden luotettavuuden ja saatavuuden. Carp otettaisiin käyttöön strategisesti tärkeiden verkkosegmenttien ja palveluiden välillä. Toimistoympäristössä kohteita olisivat sisäinen dns, sähköpostipalvelin ja Ent_cpe kytkin, joka toimii yhdyskäytävänä muille verkoille. Varastoympäristössä Br_Cpe kytkin ja Guard_pc.

Carp toteutus alkaisi laitteiston konfiguroinnilla, mikä edellyttäisi redundantteja palvelimia kullekin kriittiselle palvelulle, Esimerkiksi ensisijainen dns-palvelin yhdistettäisiin varapalvelimeen, joka on konfiguroitu samoilla dns-tietuilla ja toimialueen konfiguraatiolla.

Molemmat palvelimet liitetään samaan Carp-ryhmään jaetulla virtuaalisella IP-osoitteella, mikä varmistaa dns-kyselyt ja todennuspyynnöt voidaan käsitellä riippumatta siitä, kumpi fyysinen palvelin on toiminnassa. Verkkokonfigurointiin kuuluisi virtuaalisen IP-osoitteiden määrittäminen kullekin Carp-ryhmälle ja niihin liittyvien kytkimien ja reitittimien konfigurointi Carp-liikenteen asianmukaiseksi käsittelemiseksi. Kytkimet voidaan konfiguroida Carp-ryhmässä, jossa virtuaalinen IP-osoite toimisi sisäisten verkkojen oletuskäytävänä varmistaen jatkuvan ulkoisen yhteyden, vaikka yhteen reunalaitteeseen tulisi vika.

1.3 Tietoturva-analyysi

Carp:n käyttöönotto juustomarketin verkossa parantaisi tietoturvaa puuttumalla nykyisessä verkkoarkkitehtuurissa ilmeneviin ongelmiin. Carp poistaisi yksittäisiä vikaantumiskohtia, jotka voisivat eristää kokonaisia verkkosegmenttejä ulkoisesta yhteydestä. Carp:n konfigurointi laitteille juustomarket varmistaisi jatkuvan verkon saatavuuden myös laitteistovikojen tai huoltotoimimien aikana.

Tietoturvan kannalta Carp tarjoaa suojan tietyntyyppisiltä palvelunestohyökkäyksiltä. Jos hyökkääjä yrittää ylikuormittaa tietyn palvelimen tai reitittimen, Carp:n redundantti rakenne mahdollistaa liikenteen automaattisen uudelleenohjauksen toiminnassa oleviin varajärjestelmiin, jotta juustomarketin toiminta voisi jatkua hyökkäyksestä huolimatta. Ominaisuus on tärkeä, koska labrassa on simuloitu hacker kone, joka mahdollisesti voi kohdistaa hyökkäyksen juustomarketin järjestelmiin. Carp parantaa tietoturvaa parantamalla laitteistopohjaisten haavoittuvuuksien sietokykyä.

Verkossa on useita kriittisiä laitteita esimerkiksi sisäinen dns, joista puuttuu redundanssi. Jos jokin järjestelmistä kokisi laitevian tai laite olisi poissa käytöstä. Carp toteutus varmistaisi, että varajärjestelmät olisivat välittömästi valmiita jatkamaan ja ylläpitää laitteen toimintaa samalla, kun yhtiön tietoturvatiimi käsittelee järjestelmässä esiintynyttä vikaa. Tämä mahdollistaa aiempaa paremmalla tasolla olevan redundanssin, joka olisi liiketoiminnan kannalta kriittistä.

Asianmukaiseen konfiguraatioon tulee ottaa huomioon Carp:n tietoturvan hallinta. Carp-ryhmissä käytetty jaettu salattu tallennustila on suojattava vankasti turvallisten tallennus- ja siirtokäytäntöjen avulla. Verkonvalvojien on varmistettava, että tietoturvamäärityksen ja suojaukset ovat identtiset kaikkien ryhmän jäsenten välillä, jotta vältytään tietoturvaerot vikatilanteissa.

1.4 Juustomarketin arviointi

Ottaen huomioon juustomarketin verkkoarkkitehtuurin. Carp toteutus ratkaisisi useita kriittisiä haavoittuvuuksia ja toiminnallisia haasteita juustomarketin liiketoiminnan kannalta. Carp:n mahdollisia käyttötapauksia ovat: reunareitittimen redundanssi, todennuspalvelun jatkuvuus, sähköpostiviestinnän jatkuvuus ja mahdollisten etätyöntekijöiden tuki.

Carp käyttöönotto tarjoaa jatkuvan ulkoisen yhteyden toimisto ja varasto segmenttiin. Carp suojaisi internet yhteyden häiriöiltä, jotka vosivat vaikuttaa tilausten käsittelyyn, asiakaspalveluun tai työntekijöiden viestintään.

Soveltamalla Carp:ia sisäiseen dns:ään ja domain controlleriin juustomarket varmistaisi keskeytymättömät todennuspalvelut käyttäjille koko organisaatiotasolla. Käyttöönotto estäisi tilanteet, joissa työntekijät eivät voi käyttää tarvittavia järjestelmiä vikojen vuoksi.

Carpin käyttöönotto sähköpostipalvelimella takaisi jatkuvan sähköpostiviestinnän, joka on tärkeää yrityksen sisäiselle viestinnälle ja asiakaspalvelussa. Sähköposti palvelimen vika vaikuttaisi kriittisesti yrityksen kommunikaatioon ja toimintoihin. Carp tarjoaa ratkaisun, jossa viasta huolimatta palvelut pysyvät toiminnassa.

1.5 Yhteenveto

Carp tarjoaa juustomarketille tehokkaan ratkaisun verkon luotettavuuden ja turvallisuuden parantamiseksi. Carp:n toteuttaminen kriittisille palveluille voi juustomarket jatkaa liiketoimintaansa, vaikka jokin laite sammuisi. Carp suojaa myös erilaisia tietoturvahyökkäyksiä vastaan varmistaen liiketoiminnan jatkuvuus. Carp tarjoaa juustomarketille lisää verkon sietokykyä ja tarjoaisi mahdollisille tulevaisuuden kasvulle alustan kasvaa. Carp käyttöönotto vaatii aluksi investointeja, jotta se saadaan toimimaan. Operatiiviset hyödyt ja liiketoiminnan turvaaminen vikatilanteissa tarjoavat yritykselle houkuttelevan vaihtoehdon, jota juustomarketin johdon tulisi vakavasti miettiä.

1.6 Lähteet

OpenBsd dokumentti. (2024).” Firewall Redundancy CARP and pfsync”. Saatavilla: https://www.openbsd.org/faq/pf/carp.html [viitattu 30.5.2025]

Linux dokumentti. (2024). "CARP your way to high availability." Saatavilla: https://www.linux.com/news/carp-your-way-high-availability/ [viitattu 30.5.2025]