Isaacus

Table of Contents

[1. Ympäristökuvaus 2](#_Toc512522499)

[2. Toiminta 2](#_Toc512522500)

[3. Guacamole 2](#_Toc512522501)

[4. Guacamolen asennus 2](#_Toc512522502)

[5. Guacamolen konfigurointi 5](#_Toc512522503)

[6. Web -palvelimen konfigurointi 7](#_Toc512522504)

[7. Palomuurin konfigurointi 7](#_Toc512522505)

[8. Windows-ympäristö 7](#_Toc512522506)

[a. Isaacusdc1 8](#_Toc512522507)

[b. Isaacusdc2 11](#_Toc512522508)

[c. ISAACUSCB1 19](#_Toc512522509)

[d. Isaacusgw1 20](#_Toc512522510)

[e. ISAACUSFS 21](#_Toc512522511)

[9. Linux-ympäristö 23](#_Toc512522512)

[a. isaacusipa1 23](#_Toc512522513)

[b. isaacusipa2 25](#_Toc512522514)

[c. isaacussw1 25](#_Toc512522515)

[d. Linux-palvelimen konfigurointi spacewalk-asiakkaaksi 27](#_Toc512522516)

[e. Linux-palvelimen konfigurointi ipa-asiakkaaksi 27](#_Toc512522517)

[f. isaacusmfa 28](#_Toc512522518)

[10. Linux -työpöytien konfiguraatio 34](#_Toc512522519)

[11. SFTP -palvelin 34](#_Toc512522520)

[12. Tekninen ympäristökuvaus 36](#_Toc512522521)

[Palvelinluettelo 36](#_Toc512522522)

# Ympäristökuvaus

Isaacuksen kiinteä ympäristö koostuu 15 virtuaalipalvelimesta, jotka on toteutettu CSC:n vCloud-alustalla. Kuuden palvelimen käyttöjärjestelmä on Windows Server 2016, ja yhdeksän palvelimen käyttöjärjestelmä on CentOS 7. vCloud-ympäristön verkkokonteksti on 193.166.16.128/26. vCloud-ympäristön palvelimet ovat ns. pysyviä palvelimia, joita tarvitaan jatkuvasti ympäristön toimimiseksi. CSC:n ePouta-pilvialustalla on toteutettu ei-pysyviä palvelimia, joita ovat käyttäjien työpöytäpalvelimet. ePouta-palvelinten käyttöjärjestelminä käytetään Windows Server 2016:sta ja CentOS 7:ää, ja ympäristön verkkokonteksti on 192.168.30.0/24. vCloud ja ePouta –ympäristöt on yhdistetty toisiinsa CSC:n konesaliverkon kautta. vCloudissa liikennettä rajoittaa verkon palomuuri ja ePoudassa instanssikohtaiset Security Groupit.

# Toiminta

Järjestelmän käyttäjät yhdistävät selaimellaan Guacamole- (<https://eta.csc.fi/guacamole/)> tai RD Web –palvelimeen (https://gw.eta.csc.fi) ja kirjautuvat sisään heille annetuilla tunnuksilla. Tunnukset on tallennettu Active Directory –palvelinten LDAP-kantaan ja lisäksi käytettävän Guacamole-palvelimen MariaDB-tietokantaan.

Kirjautumisen jälkeen käyttäjä valitsee palvelimen tai farmin, johon hän haluaa yhdistää. Mikäli käyttäjällä on oikeus kirjautua vain yhdelle palvelimelle ja hän käyttää Guacamolea, yhdistetään hänet suoraan palvelimelle. Käyttäjän laitteelta vaaditaan ainoastaan moderni HTML 5:ttä tukeva selain. Palvelimelle yhdistämisen jälkeen käyttäjältä vaaditaan vielä kaksivaiheinen tunnistautuminen.

# Guacamole

Isaacus käyttää Apachen avoimen lähdekoodin ilmaista Guacamole -tuotetta, joka mahdollistaa etäyhteyden (RDP, VNC, SSH, Telnet) muodostamisen pelkkää selainta käyttämällä. Guacamolea ylläpidetään CSC:n omalla virtuaalipalvelimella (CentOS 7). Guacamole toimii Apache Tomcatin ja HTTP -palvelimen avulla. Guacamole on avointa lähdekoodia (<https://github.com/apache/guacamole-server>, https://github.com/apache/guacamole-client)

# Guacamolen asennus

Guacamolea ja RDP-yhteyksiä varten tarvitaan seuraavat paketit:

* Cairo-devel
* libjpeg-turbo-devel
* libpng-devel
* uuid-devel
* freerdp-devel
* openssl-devel
* libwebp-devel
* tomcat
* tomcat-admin-webapps
* tomcat-webapps
* autoconf
* automake
* libtool

Guacamolen palvelinosa asennetaan lataamalla haluttu versio .tar.gz -pakettina, purkamalla se haluttuun sijaintiin ja ajamalla hakemiston sisältä tarvittavat asennuskomennot:

*tar -xf guacamole-server-0.9.14.tar.gz  
cd guacamole-server-0.9.14/  
./configure --with-init-dir=/etc/init.d  
make  
make install  
ldconfig*

Guacamolen client -osan asentamiseksi riittää guacamole.war -tiedoston kopioiminen Tomcatin webapps-hakemistoon (/*usr/share/tomcat/webapps/)* guacamole.war-nimellä.

LDAP -tukea varten Guacamole tarvitsee MySQL-tietokannan, johon se tallentaa tiedot olemassa olevista yhteyksistä ja siitä, mitä oikeuksia käyttäjillä on. MySQL-tietokantana voidaan käyttää MariaDB:tä tai MySQL:ää, molemmat toimivat yhtä hyvin. Joka tapauksessa tietokannan asentamisen jälkeen on syytä ajaa mysql\_secure\_installation. Lisäksi tarvitaan MySQL -ajuri JDBC:lle sekä Guacamolen MySQL -lisäosa. SQL:ään luodaan Guacamolelle tietokanta ja käyttäjä, sekä annetaan käyttäjälle tarvittavat oikeudet:

*mysql -u root -p  
  
CREATE DATABASE guacamole\_db;  
CREATE USER 'guacamole\_user'@'localhost' IDENTIFIED BY ‘<password>’;  
GRANT SELECT,INSERT,UPDATE,DELETE ON guacamole\_db.\* TO 'guacamole\_user'@'localhost';  
FLUSH PRIVILEGES;  
quit*

Lopuksi ajetaan vielä Guacamolen skeema tietokantaan. Tarvittavat .sql-tiedostot löytyvät MySQL-lisäosan hakemistosta mysql/schema. Alla oleva komento on ajettu mysql-kansiosta:

*cat schema/\*.sql | mysql -u root -p guacamole\_db*

MySQL -lisäosa asennetaan kopioimalla lisäosa Guacamolen extensions-hakemistoon ja ajuri Guacamolen lib-hakemistoon:

*mkdir /usr/share/tomcat/.guacamole  
mkdir /usr/share/tomcat/.guacamole/extensions  
cp guacamole-auth-jdbc-0.9.14/mysql/guacamole-auth-jdbc-mysql-0.9.14-incubating.jar /usr/share/tomcat/.guacamole/extensions/  
mkdir /usr/share/tomcat/.guacamole/lib  
cp mysql-connector-java-5.1.42/mysql-connector-java-5.1.42-bin.jar /usr/share/tomcat/.guacamole/lib/*

Guacamolen aseuksia muokataan asetustiedostosta */usr/share/local/tomcat/.guacamole/guacamole.properties:*

*#* [*MySQL*](https://wiki.csc.fi/bin/edit/KAMUT/MySQL?topicparent=KAMUT.ISAACUSLAULUJOUTSEN) *properties  
mysql-hostname: localhost  
mysql-port: 3306  
mysql-database: guacamole\_db  
mysql-username: guacamole\_user  
mysql-password: yourpassword*

Asetusten muokkaamisen jälkeen Tomcat on käynnistettävä uudelleen. Guacamolen skeematiedosto luo automaattisesti ylläpitäjän oikeuksilla varustetun käyttäjän, jonka tunnus on guacadmin ja salasana guacadmin. Tunnuksen salasana on syytä vaihtaa kirjautumalla Guacamoleen web -sovelluksen kautta ja vaihtamalla salasana käyttäjän asetuksista.

LDAP-lisäosa hyödyntää jo asennettua MySQL -tietokantaa, ja sen asentamiseksi riittää lisäosan kopiointi Guacamolen extensions -hakemistoon ja Guacamolen asetusten muokkaaminen:

*# LDAP properties  
ldap-hostname: isaacusdc1.rothovius.local  
ldap-port: 389  
ldap-user-base-dn: OU=TestUsers,DC=Isaacus,DC=local  
ldap-username-attribute: CN  
ldap-config-base-dn: OU=TestUsers,DC=Isaacus,DC=local*

*Ldap-user-base-dn* –kohdassa määritellystä OU:sta täytyy löytyä käyttäjätunnus, jolla on sama nimi kuin Guacamolen omassa tietokannassa olevalla ylläpitäjän oikeuksilla varustetulla tunnuksella (käytännössä esimerkiksi automaattisesti luotu guacadmin-tunnus). Yllä olevilla asetuksilla Guacamolea voidaan käyttää ainoastaan määritellyssä OU:ssa olevilla käyttäjätunnuksilla, alakansioissa olevat tunnukset eivät toimi. Mikäli asetuksiin määrittelee *ldap-search-bind-dn* –rivillä käyttäjätunnuksen ja *ldap-search-bind-password* –rivillä salasanan, voi Guacamole käyttää määriteltyä tunnusta käyttäjien hakemiseen myös user-base –kansion alakansioista.

Kirjautumissivua voi kustomoida luomalla oman Guacamole -lisäosan. Lisäosan rakenne on seuraava:

*ext/guac-manifest.json*

*ext/loginDisclaimer.html*

*ext/css/login-override.css*

*ext/translations/en.json*

Lisäksi *ext/resources* –hakemistoon sijoitetaan tarvittavat kuvat. Tiedostojen sisältö on raportin liitteenä. Tiedostot pakataan yhteen .jar-tiedostoon (*zip –r lisaosa.jar \**) ja .jar-tiedosto siirretään Guacamolen extensions -hakemistoon ja käynnistetään Tomcat uudelleen.

# Guacamolen konfigurointi

Uusia yhteyksiä luodaan asetusten Connections -välilehdellä. Esimerkkinä Helsingin Yliopiston käyttämä yhteys:

*Name: HY  
Location: ROOT*

*Protocol: RDP*

*Maximum number of connections: 50*

*Maximum number of connections per user: 10 (tällä ei ole suurtakaan merkitystä, mutta yhteyksiä on hyvä sallia useampi siltä varalta, että vanha yhteys jää roikkumaan)*

*Guacamole Proxy Parameters jätetään tyhjäksi*

*Hostname: isaacusrd1.isaacus.local (kun välissä on RD Connection Broker, farmiin yhdistää minkä tahansa farmin koneen nimellä, ja Broker jakaa yhteydet farmin koneiden kesken tästä huolimatta)*

*Port: 3389*

*Username: ${GUAC\_USERNAME} (Linux-palvelimella ${GUAC\_USERNAME}@isaacus.local)*

*Password: ${GUAC\_PASSWORD}*

*Domain: Isaacus.local*

*Security Mode: NLA*

*Ignore Server Certificate*

*Keyboard layout: Swedish (Qwerty)*

*Resize method: Display Update*

*Enable wallpaper*

Yhteyden luomisen jälkeen käyttäjälle annetaan oikeus yhteyden käyttämiseen käyttäjän asetuksista valitsemalla halutut yhteydet Connections -kohdassa. Oikeudet yhteyksien käyttämiseen voidaan myös kirjoittaa suoraan Guacamolen tietokantaan. Koska Guacamole tallentaa tietokantaansa käyttäjätunnukset ainoastaan, mikäli niille tehdään jotakin muutoksia (esimerkiksi annetaan oikeus käyttää jotakin yhteyttä), täytyy tällöin oikeuksien lisäksi myös tunnukset kirjoittaa tietokantaan. Käytännössä pienillä käyttäjämäärillä yhteyksien määrittäminen käyttäjille on vielä toimiva vaihtoehto, mutta käyttäjämäärien kasvaessa tietokannan muokkaaminen suoraan on huomattavasti nopeampi vaihtoehto.

*Guacamole\_user* –tauluun kirjoitetaan kentille *username, password\_salt, password\_hash ja password\_date* sopivat tiedot. *Password\_salt* ja *password\_hash* muodostuvat annetun salasanan perusteella. Salasanan ei tarvitse (eikä adminin edes pitäisi salasanaa tietää) olla käyttäjän oikea salasana, koska autentikointi tapahtuu joka tapauksessa LDAPin kautta. Kun tunnus on kirjoitettu tietokantaan, kirjoitetaan *guacamole\_connection\_permission* –taulun kenttiin *user\_id, connection\_id* ja *permission* sopivat arvot. Käyttäjien lisäämistä ja yhteysoikeuksien asettamista varten tarvittavien SQL -komentojen generoimista varten on kirjoitettu skriptit createUsers.sh ja assignConnections.sh.

Mikäli tiedostonsiirtoa käyttäjän ja etätyöpöydän välillä ei haluta sallia, otetaan valinta pois *Enable drive* –kohdasta. Leikepöydän käytön estäminen Windows-työpöydillä tapahtuu Server Collectionin asetuksista, mutta Linux -työpöytien leikepöydän estäminen vaatii cliprdr-tuen rikkomista Guacamole -palvelimen Freerdp:stä. Tämä tapahtuu uudelleennimeämällä tai poistamalla guacdr -nimiset tiedostot /usr/local/lib, /usr/local/lib64, /usr/local/lib/freerdp ja /usr/local/lib64/freerdp –hakemistoista ennen Guacamole serverin asennusta.

# Web -palvelimen konfigurointi

Apache Web Serverillä on konfiguroitu SSL sekä ProxyPass ja uudelleenohjaukset niin, että Guacamolen etusivulle pääsee suoraan ilman porttien tai polkujen määrittelyjä selaimessa. ProxyPass on konfiguroitu myös WebSocketille. Konfiguraatiotiedostot liitteenä (/etc/httpd/conf.d/guacamole.conf) /etc/httpd/conf.d/ssl.conf-tiedostossa on kommentoitu pois rivi *Listen 443 https*.

# Palomuurin konfigurointi

Isaacuksen Linux-palvelimilla on käytössä Firewalld. Palomuurissa on avattu portit 8080/tcp, 8443/tcp. Lisäksi CSC:n palomuurista on lähtökohtaisesti estetty kaikki yhteydet, ja sallittu käyttäjien ilmoittamat IP-osoitteet erikseen. Käyttäjien IP -osotteista on sallittu ainoastaan portti 443 tarvittavaan Guacamole -palvelimeen.

# Windows-ympäristö

Windows-palvelimet on liitetty ISAACUS.local-domainiin. Ympäristön Domain Controller –palvelimiksi on asennettu ISAACUSDC1 ja ISAACUSDC2. DC-palvelimet toimivat myös ympäristön sisäisinä DNS-palvelimina. ISAACUSDC2-palvelin toimii myös WSUS-palvelimena, joka hakee Microsoftilta Windows-päivityksiä ja tarjoaa niitä ympäristön muille Windows-koneille. ISAACUSGW1-palvelin toimii Remote Desktop Gateway –palvelimena sekä RD Web –palvelimena. RD Web on toteutettu Microsoftin uuden HTML 5 –sovelluksen esiversiolla (<https://cloudblogs.microsoft.com/enterprisemobility/2018/03/28/remote-desktop-web-client-public-preview/)>. ISAACUSCB1-palvelin toimii RD-ympäristön Connection Brokerina.

# Isaacusdc1

*# Rename computer and set DNS*

*Rename-Computer -newname ISAACUSDC1*

*Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses "<isaacusdc2>,<isaacusdc1>"*

*Restart-Computer*

*Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ResetServerAddresses*

*# Install Roles*

*Install-WindowsFeature AD-Domain-Services -IncludeManagementTools*

*Import-Module ADDSDeployment*

*Install-ADDSForest `*

*-CreateDnsDelegation:$false `*

*-DatabasePath "C:\Windows\NTDS" `*

*-DomainMode "WinThreshold" `*

*-DomainName "ISAACUS.local" `*

*-DomainNetbiosName "ISAACUS" `*

*-ForestMode "WinThreshold" `*

*-InstallDns:$true `*

*-LogPath "C:\Windows\NTDS" `*

*-NoRebootOnCompletion:$false `*

*-SysvolPath "C:\Windows\SYSVOL" `*

*-Force:$true*

*# Add DNS Forwarders*

*Add-DnsServerForwarder -IPAddress 193.166.4.24 -PassThru*

*Add-DnsServerForwarder -IPAddress 193.166.4.25 -PassThru*

*# Check services*

*Get-Service adws,kdc,netlogon,dns*

*Get-Smbshare*

*# Check logs*

*get-eventlog "Directory Service" | select entrytype, source, eventid, message*

*get-eventlog "Active Directory Web Services" | select entrytype, source, eventid, message*

*# Remove CD drive letter*

*$drive = gwmi win32\_volume -Filter "DriveLetter = 'd:'"*

*Set-WmiInstance -input $drive -Arguments @{DriveLetter=$null;Label=$newReplayName}*

*# Format datadisk*

*Initialize-Disk -Number 1*

*Get-Disk -Number 1 | New-Partition -UseMaximumSize -DriveLetter D | Format-Volume -FileSystem NTFS -NewFileSystemLabel "Data" -Confirm:$Fals*

*# Scavenging and aging*

*Set-DnsServerScavenging –ScavengingState $True –ScavengingInterval 7:00:00:00 -RefreshInterval 1.00:00:00 –ApplyOnAllZones*

*Set-DnsServerZoneAging isaacus.local -Aging $True*

*# Allow zone transfers, only to servers listed on the Name Servers tab*

*Set-DnsServerPrimaryZone -Name ISAACUS.local -SecureSecondaries TransferToZoneNameServer -PassThru*

*# Install DHCP Server*

*Install-WindowsFeature DHCP -IncludeManagementTools*

*Add-DHCPServerSecurityGroup -ComputerName ISAACUSDC1*

*Add-DhcpServerInDC -DnsName ISAACUSDC1.ISAACUS.local -IPAddress <isaacusdc1>*

*Get-DhcpServerInDC*

*Add-DhcpServerv4Scope -name "ISAACUS" -StartRange <ip> -EndRange <ip> -SubnetMask <mask> -State Active*

*Set-DHCPServerv4OptionValue -ComputerName ISAACUSDC1.ISAACUS.local -DnsServer <isaacusdc1>,<isaacusdc2> -DnsDomain ISAACUS.local -Router <ip>*

*#Needed to commit authorization in gui Post-Install configuration wizard. Authorizing DHCP failed because the server was already present in the active directory.*

*#Install DFS*

*Install-WindowsFeature FS-DFS-Namespace, RSAT-DFS-Mgmt-Con*

*# Create the SMB share folders:*

*New-Item "D:\DFSRoots\Files" –type directory # Create the shares*

*New-SMBShare –Name “Files” –Path “D:\DFSRoots\Files” `*

*–FullAccess "ISAACUS\Domain Admins" `*

*-ChangeAccess "ISAACUS\Domain Users"*

*# Create the DFS Root*

*New-DfsnRoot -Path \\ISAACUS.local\files -TargetPath \\ISAACUSDC1\files -Type DomainV2*

*New-DfsnFolderTarget -Path "\\ISAACUS.local\Files\data\" -TargetPath "\\ISAACUSFS\data"*

*New-DfsnFolderTarget -Path "\\ISAACUS.local\Files\UPD$\" -TargetPath "\\ISAACUSFS\UPD$"*

*New-DfsnFolderTarget -Path "\\ISAACUS.local\Files\Admin\" -TargetPath "\\ISAACUSFS\Admin"*

*# Others*

*# Disable IPv6*

*Get-NetAdapterBinding*

*Disable-NetAdapterBinding –InterfaceAlias “Ethernet0” –ComponentID ms\_tcpip6*

# Isaacusdc2

*# Rename, set dns and join domain*

*Rename-computer -newname ISAACUSDC2*

*Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses "<isaacusdc1>,<isaacusdc2>"*

*Add-Computer -DomainName ISAACUS.local -Credential $(get-credential)*

*Restart-Computer*

*Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ResetServerAddresses*

*# Install ADDS*

*Import-Module ADDSDeployment*

*Install-ADDSDomainController `*

*-NoGlobalCatalog:$false `*

*-CreateDnsDelegation:$false `*

*-Credential (Get-Credential) `*

*-CriticalReplicationOnly:$false `*

*-DatabasePath "C:\Windows\NTDS" `*

*-DomainName "ISAACUS.local" `*

*-InstallDns:$true `*

*-LogPath "C:\Windows\NTDS" `*

*-NoRebootOnCompletion:$false `*

*-SiteName "Default-First-Site-Name" `*

*-SysvolPath "C:\Windows\SYSVOL" `*

*-Force:$true*

*# Server rebooting automatically*

*# DNS SETTINGS*

*# DNS alias for wsus in dns:*

*Add-DnsServerResourceRecordCName -Name "wsus" -HostNameAlias "ISAACUSDC2.ISAACUS.local" -ZoneName "ISAACUS.local"*

*# DNS Set Scavenging and aging*

*Set-DnsServerScavenging –ScavengingState $True –ScavengingInterval 7:00:00:00 -RefreshInterval 1.00:00:00 –ApplyOnAllZones*

*Set-DnsServerZoneAging isaacus.local -Aging $True*

*# Add DNS Forwarders*

*Add-DnsServerForwarder -IPAddress 193.166.4.24 -PassThru*

*Add-DnsServerForwarder -IPAddress 193.166.4.25 -PassThru*

*# Check services*

*Get-Service adws,kdc,netlogon,dns*

*Get-Smbshare*

*# Check logs*

*get-eventlog "Directory Service" | select entrytype, source, eventid, message*

*get-eventlog "Active Directory Web Services" | select entrytype, source, eventid, message*

*# Remove CD driver letter*

*$drive = gwmi win32\_volume -Filter "DriveLetter = 'd:'"*

*Set-WmiInstance -input $drive -Arguments @{DriveLetter=$null;Label=$newReplayName}*

*#Format datadisk*

*Initialize-Disk -Number 1*

*Get-Disk -Number 1 | New-Partition -UseMaximumSize -DriveLetter D | Format-Volume -FileSystem NTFS -NewFileSystemLabel "Data" -Confirm:$False*

*# WSUS INSTALL*

*#INSTALL WSUS*

*Install-WindowsFeature -Name UpdateServices -IncludeManagementTools*

*New-Item -Path D: -Name WSUS -ItemType Directory*

*C:\'Program Files'\'Update Services'\Tools\wsusutil.exe postinstall CONTENT\_DIR=D:\WSUS*

*Set-WsusServerSynchronization –SyncFromMU*

*# Get WSUS Server Object*

*$wsus = Get-WSUSServer*

*# Connect to WSUS server configuration*

*$wsusConfig = $wsus.GetConfiguration()*

*# Set Update Languages to English and save configuration sett*

*$wsusConfig.AllUpdateLanguagesEnabled = $false*

*$wsusConfig.SetEnabledUpdateLanguages(“en”)*

*$wsusConfig.Save()*

*# Get WSUS Subscription and perform initial synchronization to get latest categories*

*$subscription = $wsus.GetSubscription()*

*$subscription.StartSynchronizationForCategoryOnly()*

*write-host 'Beginning first WSUS Sync to get available Products etc' -ForegroundColor Magenta*

*write-host 'Will take some time to complete'*

*While ($subscription.GetSynchronizationStatus() -ne 'NotProcessing') {*

*Write-Host "." -NoNewline*

*Start-Sleep -Seconds 5*

*}*

*write-host ' '*

*Write-Host "Sync is done." -ForegroundColor Green*

*# Configure the Platforms that we want WSUS to receive updates*

*# First disable all products*

*write-host 'Diabling products WSUS Products'*

*Get-WsusProduct | Set-WsusProduct -Disable*

*# Enable the ones you need*

*write-host 'Setting WSUS Products'*

*Get-WsusProduct | where-Object {*

*$\_.Product.Title -in (*

*'Windows Server 2016 and Later Servicing Drivers',*

*'Windows Server 2016',*

*'Windows Server Manager – Windows Server Update Services (WSUS) Dynamic Installer')*

*} | Set-WsusProduct*

*# Configure Synchronizations*

*write-host 'Enabling WSUS Automatic Synchronisation'*

*$subscription.SynchronizeAutomatically=$true*

*# Set synchronization scheduled for midnight each night*

*$subscription.SynchronizeAutomaticallyTimeOfDay= (New-TimeSpan -Hours 0)*

*$subscription.NumberOfSynchronizationsPerDay=12*

*$subscription.Save()*

*# Kick off a synchronization*

*$subscription.StartSynchronization()*

*# Monitor Progress of Synchronisation*

*write-host 'Starting WSUS Sync, will take some time' -ForegroundColor Magenta*

*Start-Sleep -Seconds 60 # Wait for sync to start before monitoring*

*while ($subscription.GetSynchronizationProgress().ProcessedItems -ne $subscription.GetSynchronizationProgress().TotalItems) {*

*Write-Progress -PercentComplete (*

*$subscription.GetSynchronizationProgress().ProcessedItems\*100/($subscription.GetSynchronizationProgress().TotalItems)*

*) -Activity "WSUS Sync Progress"*

*}*

*Write-Host "Sync is done." -ForegroundColor Green*

*# Configure Default Approval Rule*

*if ($DefaultApproval -eq $True)*

*{*

*write-host 'Configuring default automatic approval rule'*

*[void][reflection.assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")*

*$rule = $wsus.GetInstallApprovalRules() | Where {*

*$\_.Name -eq "Default Automatic Approval Rule"}*

*$class = $wsus.GetUpdateClassifications() | ? {$\_.Title -In (*

*'Critical Updates',*

*'Definition Updates',*

*'Feature Packs',*

*'Security Updates',*

*'Service Packs',*

*'Update Rollups',*

*'Updates')}*

*$class\_coll = New-Object UpdateClassificationCollection*

*$class\_coll.AddRange($class)*

*$rule.SetUpdateClassifications($class\_coll)*

*$rule.Enabled = $True*

*$rule.Save()*

*}*

*# Configure Default Approval Rule*

*$wsus = Get-WSUSServer*

*$DefaultApproval = $True*

*if ($DefaultApproval -eq $True)*

*{*

*write-host 'Configuring default automatic approval rule'*

*[void][reflection.assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")*

*$rule = $wsus.GetInstallApprovalRules() | Where {*

*$\_.Name -eq "Default Automatic Approval Rule"}*

*$class = $wsus.GetUpdateClassifications() | ? {$\_.Title -In (*

*'Critical Updates',*

*'Definition Updates',*

*'Feature Packs',*

*'Security Updates',*

*'Service Packs',*

*'Update Rollups',*

*'Updates')}*

*$class\_coll = New-Object UpdateClassificationCollection*

*$class\_coll.AddRange($class)*

*$rule.SetUpdateClassifications($class\_coll)*

*$rule.Enabled = $True*

*$rule.Save()*

*}*

*# Run Default Approval Rule*

*$RunDefaultRule = $True*

*if ($RunDefaultRule -eq $True)*

*{*

*write-host 'Running Default Approval Rule'*

*write-host ' >This step may timeout, but the rule will be applied and the script will continue' -ForegroundColor Yellow*

*try {*

*$Apply = $rule.ApplyRule()*

*}*

*catch {*

*write-warning $\_*

*}*

*Finally {*

*write-host 'WSUS log files can be found here: %ProgramFiles%\Update Services\LogFiles'*

*write-host 'Done!' -foregroundcolor Green*

*}*

*}*

*#Add DNS alias for wsus in dns:*

*Add-DnsServerResourceRecordCName -Name "wsus" -HostNameAlias "ISAACUSDC2.ISAACUS.local" -ZoneName "ISAACUS.local"*

*WSUS Reporting needs:*

*Install Microsoft Report Viewer 2012 with default settings.*

*https://www.microsoft.com/en-ca/download/details.aspx?id=35747*

*Microsoft System CLR Types for Microsoft SQL Server 2012 with default settings.*

*http://go.microsoft.com/fwlink/?LinkID=239644&clcid=0x409*

*Others*

*# MOVE FSMO INFRASTRUCTURE ROLE TO ISAACUSDC2*

*FSMO infrastructure role to ISAACUSDC2 (Move-ADDirectoryServerOperationMasterRole -Identity ISAACUSDC2.local -OperationMasterRole InfrastructureMaster)*

*# DISABLE IPV6*

*Get-NetAdapterBinding*

*Disable-NetAdapterBinding –InterfaceAlias “Ethernet0” –ComponentID ms\_tcpip6*

# ISAACUSCB1

*# Rename computer, set dns and join domain*

*Rename-Computer -newname ISAACUSCB1*

*Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses "<isaacusdc1>,<isaacusdc2>"*

*Add-Computer -DomainName ISAACUS.local -Credential $(get-credential)*

*Restart-Computer*

*Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ResetServerAddresses*

*# Remove CD drive letter*

*$drive = gwmi win32\_volume -Filter "DriveLetter = 'd:'"*

*Set-WmiInstance -input $drive -Arguments @{DriveLetter=$null;Label=$newReplayName}*

*# Install Remote Desktop Services*

*Add-WindowsFeature Remote-Desktop-Services,RDS-Connection-Broker,RDS-Licensing,RDS-RD-Server,RSAT-RDS-Tools,RSAT-RDS-Gateway,RDS-Licensing-UI -IncludeManagementTools*

*Restart-Computer*

*# Create New Session Deployment*

*Import-Module RemoteDesktop*

*New-RDSessionDeployment -ConnectionBroker ISAACUSCB1.ISAACUS.local -WebAccessServer ISAACUSGW1.ISAACUS.local -SessionHost ISAACUSRD1.ISAACUS.local*

*# Gateway Settings*

*Add-RDServer -Server ISAACUSGW1.ISAACUS.LOCAL -Role RDS-GATEWAY -ConnectionBroker ISAACUSCB1.ISAACUS.LOCAL -GatewayExternalFqdn gw.eta.csc.fi*

*Set-RDDeploymentGatewayConfiguration -GatewayMode Automatic*

*# Rename RDWorkspace (Description)*

*Set-RDWorkspace -Name "ISAACUS"*

*# Create new session collection*

*New-RDSessionCollection -CollectionName "ISAACUSTEST01" -SessionHost ISAACUSRD1.ISAACUS.local -CollectionDescription "ISAACUS" -ConnectionBroker ISAACUSCB1.ISAACUS.local*

*Set-RDSessionCollectionConfiguration -CollectionName "ISAACUSTEST01" -ClientDeviceRedirectionOptions None -ConnectionBroker "ISAACUSCB1.ISAACUS.local"*

*# Add Servers to Server Manager*

*# Add servers via GUI: Server Manager → Manage → Add servers → Find now → Add all servers OR run add\_servers\_to\_servermanager.ps1*

# Isaacusgw1

*# Join domain*

*Add-Computer -DomainName ISAACUS.local -Credential $(get-credential)*

*Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses "<isaacusdc1>,<isaacusdc2>"*

*Restart-Computer*

*# Remove CD drive letter*

*$drive = gwmi win32\_volume -Filter "DriveLetter = 'd:'"*

*Set-WmiInstance -input $drive -Arguments @{DriveLetter=$null;Label=$newReplayName}*

*# Installing the HTML5 RDP client*

*# https://cloudblogs.microsoft.com/enterprisemobility/2018/03/28/remote-desktop-web-client-public-preview/*

*# https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-web-client-admin*

*# You will need Internet access for this*

*Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force*

*Install-Module -Name PowerShellGet -Force*

*# Restart Powershell*

*Install-Module -Name RDWebClientManagement*

*Install-RDWebClientPackage*

*Import-RDWebClientBrokerCert "C:\brokercert\isaacuscb1RDCert.cer"*

*Publish-RDWebClientPackage -Type Production -Latest*

*# Find your new HTML5 client at:* [*https://isaacusgw1.isaacus.local/RDWeb/pages/webclient/*](https://isaacusgw1.isaacus.local/RDWeb/pages/webclient/)

RD Gateway Managerin asetuksissa lisätään tarvittavat Resource Access Policyt sekä Connection Access Policyt.

# ISAACUSFS

*Rename-Computer -newname ISAACUSFS*

*Reboot-Computer*

*Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses "<isaacusdc1>,<isaacusdc2>"*

*Add-Computer -DomainName ISAACUS.local -Credential $(get-credential)*

*# Remove CD drive letter*

*$drive = gwmi win32\_volume -Filter "DriveLetter = 'd:'"*

*Set-WmiInstance -input $drive -Arguments @{DriveLetter=$null;Label=$newReplayName}*

*# Format datadisk D*

*Initialize-Disk -Number 1*

*Get-Disk -Number 1 | New-Partition -UseMaximumSize -DriveLetter D | Format-Volume -FileSystem NTFS -NewFileSystemLabel "Data" -Confirm:$False*

*# Create the SMB share folders:*

*New-Item “D:\Data" –type directory*

*New-Item “D:\UPD" –type directory*

*New-Item "D:\Admin" -type directory*

*New-Item "D:\Admin\scripts" -type directory*

*#Create the shares*

*New-SMBShare –Name “Data” –Path “D:\Data” `*

*–FullAccess "ISAACUS\Domain Admins" `*

*-ChangeAccess "ISAACUS\Domain Users"*

*New-SMBShare –Name “UPD$” –Path “D:\UPD” `*

*–FullAccess "ISAACUS\Domain Admins" `*

*-ChangeAccess "ISAACUS\Domain Users"*

*New-SmbShare -Name "Admin" -Path "D:\Admin" `*

*-FullAccess "ISAACUS\Domain Admins"*

# Linux-ympäristö

Linux-palvelimet on liitetty ipa.isaacus.local-domainiin, jolla on luottosuhde ISAACUS.local-domainiin. IPA Master -palvelimina toimivat isaacusipa1 ja isaacusipa2. Windows-palvelimista poiketen Linux-palvelinten on nimetty pienillä kirjaimilla kirjoitettuna IPAn vaatimuksista johtuen. Samoin palvelinten täydellinen nimi on muotoa nimi.ipa.isaacus.local, kun Windows-palvelimilla se on nimi.isaacus.local. IPA-domainiin tuodaan luottosuhteen avulla tarvittavat käyttäjäryhmät ulkoisina ryhminä, jolloin käyttäjien pääsyä eri palvelimille voidaan hallinnoida, mutta varsinainen käyttäjienhallinta on silti keskitetty AD:hen.

Linux-palvelinten hallintaa ja päivityksiä varten on asennettu Spacewalk-palvelin isaacussw1, joka hakee palvelinten ja ohjelmistojen päivitykset Internetistä ja jakaa niitä ympäristön muille Linux-palvelimille.

Kaksivaiheista tunnistautumista varten on asennettu multiOTP-palvelin isaacusmfa, joka generoi ja synkronoi aikaan perustuvia kertakäyttösalasanoja, joita kysytään käyttäjältä etätyöpöydälle kirjautumisen yhteydessä varsinaisen tunnus-salasana-yhdistelmän lisäksi. OTP-palvelin synkronoi käyttäjätunnukset AD:sta ja luo automaattisesti TOTP-tokenit sekä QR-koodin, jolla käyttäjä voi lisätä tokenin omaan autentikaattorisovellukseensa (esim. Google Authenticator). MultiOTP on avointa lähdekoodia (<https://github.com/multiOTP/multiotp>, https://github.com/multiOTP/multiOTPCredentialProvider)

# isaacusipa1

*/etc/resolv.conf:*

*search ipa.isaacus.local*

*nameserver <isaacusipa1>*

*nameserver <isaacusipa2>*

*/etc/hosts:*

*127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4*

*<ip-osoite> isaacusipa1.ipa.isaacus.local*

*# Firewall:*

*firewall-cmd --permanent --add-service=http --add-service=https --add-service=ldap --add-service=ldaps --add-service=kerberos --add-service=kpasswd --add-service=ntp --add-service=dns*

*firewall-cmd --reload*

*mv /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.d/ssl.conf.org*

*hostnamectl set-hostname isaacusipa1.ipa.isaacus.local*

*ipa-server-install*

*DNS BIND: yes*

*host name: isaacusipa1.ipa.isaacus.local*

*domain name: ipa.isaacus.local*

*realm name: IPA.ISAACUS.LOCAL*

*# Set passwords and save to password repository*

*# Wait for installation to complete*

*cp /root/cacert.p12 /root/cacert.p12.backup*

*kinit admin*

*ipa user-find admin*

*# You should get information about the admin user as output*

*#Configure AD Trust*

*yum install -y "\*ipa-server" "\*ipa-server-trust-ad" bind bind-dyndb-ldap*

*ipa-adtrust-install --netbios-name=IPA -a <ipa admin password>*

*Trusted domains support: yes*

*ipa-sidgen task: yes*

*ipa trust-add --type=ad isaacus.local --admin <domain admin> --password*

*# Add temporarily for testing to /etc/krb5.conf under [realms] IPA.ISAACUS.LOCAL = {*

*auth\_to\_local = RULE:[1:$1@$0](^.\*@ISAACUS.local$)s/@ISAACUS.local/@isaacus.local/*

*auth\_to\_local = DEFAULT*

*systemctl restart krb5kdc sssd*

*ipa group-add --desc='Isaacus <groupname>' <groupname>\_external --external*

*ipa group-add --desc='Isaacus <groupname>' <groupname>*

*ipa group-add-member <groupname>\_external --external 'isaacus\<groupname>'*

*ipa group-add-member <groupname> --groups <groupname>\_external*

# isaacusipa2

*/etc/resolv.conf:*

*search ipa.isaacus.local*

*nameserver <isaacusipa2>*

*nameserver <isaacusipa1>*

*/etc/hosts:*

*127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4*

*<ip address> isaacusipa2.ipa.isaacus.local*

*hostnamectl set-hostname isaacusipa2.ipa.isaacus.local*

*ipa-replica-install --server=isaacusipa1.ipa.isaacus.local --domain=ipa.isaacus.local --hostname=isaacusipa2.ipa.isaacus.local --realm=IPA.ISAACUS.LOCAL --admin-password=<admin password you set up before> --setup-ca*

# isaacussw1

*# Configure Firewall*

*firewall-cmd --add-port=80/tcp --add-port=443/tcp --permanent*

*firewall-cmd --reload*

*# Setup repositories*

*https://www.itzgeek.com/how-tos/linux/centos-how-tos/how-to-install-spacewalk-on-centos-7-rhel-7.html*

*https://www.howtoforge.com/tutorial/how-to-install-spacewalk-on-centos/*

*# Setup Spacewalk repository*

*rpm -Uvh http://yum.spacewalkproject.org/2.7/RHEL/7/x86\_64/spacewalk-repo-2.7-2.el7.noarch.rpm*

*# Configure Java repositories*

*cd /etc/yum.repos.d/*

*curl -O https://copr.fedorainfracloud.org/coprs/g/spacewalkproject/java-packages/repo/epel-7/group\_spacewalkproject-java-packages-epel-7.repo*

*# Setup EPEL repo*

*rpm -Uvh https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm*

*# Install Spacewalk with PostgreSQL*

*yum install spacewalk-postgresql -y*

*yum install spacewalk-setup-postgresql -y*

*# Initialize the Database*

*postgresql-setup initdb*

*# Configure Spacewalk*

*spacewalk-setup*

*# After completed, go to https://isaacussw1.isaacus.local and set up the Spacewalk Admin User.*

*# Fix error when looking at Repo Sync status in GUI:*

*chcon -v -R --reference=/var/www/html/ /var/log/rhn/reposync/*

# Linux-palvelimen konfigurointi spacewalk-asiakkaaksi

*# Required packages: rhn-client-tools rhn-check rhn-setup rhnsd m2crypto yum-rhn-plugin rhncfg-actions*

*rpm -Uvh http://isaacussw1.isaacus.local/pub/rhn-org-trusted-ssl-cert-1.0-1.noarch.rpm*

*rhnreg\_ks --activationkey <activation key> --serverUrl https://isaacussw1.isaacus.local/XMLRPC*

*# Disable other repositories*

*yum-config-manager --disable "CentOS-7 - Base"*

*yum-config-manager --disable "Extra Packages for Enterprise Linux 7 - x86\_64"*

*yum-config-manager --disable "CentOS-7 - Extras"*

*yum-config-manager --disable "CentOS-7 - Updates"*

# Linux-palvelimen konfigurointi ipa-asiakkaaksi

*# Servername must be lower-case!*

*hostnamectl set-hostname <servername>.ipa.isaacus.local*

*/etc/resolv.conf:*

*nameserver <isaacusipa1>*

*nameserver <isaacusipa2>*

*search ipa.isaacus.local*

*/etc/hosts:*

*127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4*

*<local IP> <servername>.ipa.isaacus.local*

*yum install -y ipa-client*

*ipa-client-install --mkhomedir*

*The server will automatically discover the IPA realm, servers etc*

*# Based on http://microdevsys.com/wp/kinit-cannot-find-kdc-for-realm-while-getting-initial-credentials/*

*Edit /etc/krb5.conf:*

*dns\_lookup\_kdc = true*

*systemctl restart sssd*

# isaacusmfa

*# https://github.com/multiOTP/multiotp/wiki*

*# https://github.com/LastSquirrelIT/MultiOneTimePassword-CredentialProvider/wiki/MultiOTP*

*# Configure firewall*

*firewall-cmd --permanent --add-service=http --add-service=https*

*firewall-cmd --reload*

*yum install httpd -y*

*systemctl enable httpd*

*systemctl start httpd*

*yum install php php-fpm php-gd php-json php-mbstring php-mysqlnd php-xml php-xmlrpc php-opcache php-mbstring php-opcache php-gd php-ldap*

*# Extract the php application to webroot*

*./multiotp.php -config backend-type=files*

*./multiotp.php -config initialize-backend*

*./multiotp.php -config ldap-server-password="password\_of\_my\_ldap\_user"*

*sudo chown apache:apache /etc/multiotp/*

*# /etc/multiotp/config/multiotp.ini*

*multiotp-database-format-v3*

*; If backend is set to something different than files,*

*; and backend\_type\_validated is set to 1,*

*; only the specific information needed for the backend*

*; is used from this config file.*

*encryption\_hash=99CCFC0D033729754B6BB4832FE786A1*

*server\_secret:=dGx9cn5qeFV7fFJ5RGR/cGd4*

*actual\_version=5.1.1.2*

*admin\_password\_hash:=RGAzPSxXYhR9KVE5dScSKCcpNTxNbCIZCHM3NSpnGn0=*

*anonymous\_stat=1*

*anonymous\_stat\_last\_update=1524669924*

*anonymous\_stat\_random\_id=19241eb5584a260811cf69b5fd59b82dcfefc9e8*

*attributes\_to\_encrypt=*

*auto\_resync=1*

*backend\_encoding=UTF-8*

*backend\_type=files*

*backend\_type\_validated=0*

*cache\_data=0*

*cache\_ldap\_hash=1*

*case\_sensitive\_users=0*

*clear\_otp\_attribute=*

*console\_authentication=0*

*debug=0*

*default\_algorithm=totp*

*default\_dialin\_ip\_mask=*

*default\_user\_group=*

*default\_request\_ldap\_pwd=1*

*default\_request\_prefix\_pin=0*

*demo\_mode=0*

*developer\_mode=0*

*display\_log=1*

*domain\_name=*

*email\_admin\_address=*

*encode\_file\_id=0*

*encryption\_key\_full\_path=*

*failure\_delayed\_time=300*

*group\_attribute=Filter-Id*

*hash\_salt\_full\_path=*

*issuer=multiOTP*

*language=en*

*last\_update=1524729108*

*ldap\_expired\_password\_valid=1*

*ldap\_account\_suffix=*

*ldap\_activated=1*

*ldap\_base\_dn=DC=isaacus,DC=local*

*ldap\_bind\_dn=CN=<username>,DC=isaacus,DC=local*

*ldap\_cache\_folder=tempdir*

*ldap\_cache\_on=1*

*ldap\_cn\_identifier=sAMAccountName*

*ldap\_default\_algorithm=totp*

*ldap\_domain\_controllers=isaacusdc1.isaacus.local,isaacusdc2.isaacus.local*

*last\_failed\_white\_delay=60*

*ldap\_group\_attribute=memberOf*

*ldap\_group\_cn\_identifier=cn*

*ldap\_groups\_dn=*

*ldap\_hash\_cache\_time=604800*

*ldap\_in\_group=OTP\_Users*

*ldap\_language\_attribute=preferredLanguage*

*ldap\_network\_timeout=10*

*ldap\_port=389*

*ldap\_recursive\_cache\_only=0*

*ldap\_recursive\_groups=1*

*ldap\_server\_password: <hash of password>*

*ldap\_server\_type=1*

*ldap\_ssl=0*

*ldap\_synced\_user\_attribute=*

*ldap\_time\_limit=30*

*ldaptls\_reqcert=auto*

*ldaptls\_cipher\_suite=auto*

*log=0*

*max\_block\_failures=6*

*max\_delayed\_failures=3*

*max\_event\_resync\_window=10000*

*max\_event\_window=100*

*max\_time\_resync\_window=90000*

*max\_time\_window=600*

*multiple\_groups=0*

*ntp\_server=pool.ntp.org*

*overwrite\_request\_ldap\_pwd=1*

*radius\_error\_reply\_message=1*

*radius\_reply\_attributor= +=*

*radius\_reply\_separator\_hex=2c*

*radius\_tag\_prefix=*

*scratch\_passwords\_digits=6*

*scratch\_passwords\_amount=10*

*self\_registration=1*

*server\_cache\_level=1*

*server\_cache\_lifetime=15552000*

*server\_timeout=5*

*server\_type=xml*

*server\_url=*

*sms\_api\_id:=*

*sms\_message\_prefix=%s is your SMS-Code*

*sms\_originator=multiOTP*

*sms\_password:=*

*sms\_provider=*

*sms\_userkey:=*

*sms\_digits=6*

*sms\_timeout=180*

*smtp\_auth=0*

*smtp\_password:=*

*smtp\_port=25*

*smtp\_sender=*

*smtp\_sender\_name=*

*smtp\_server=*

*smtp\_ssl=0*

*smtp\_username=*

*sql\_server=*

*sql\_username=*

*sql\_password:=*

*sql\_database=*

*sql\_schema=*

*sql\_config\_table=multiotp\_config*

*sql\_cache\_table=multiotp\_cache*

*sql\_devices\_table=multiotp\_devices*

*sql\_groups\_table=multiotp\_groups*

*sql\_log\_table=multiotp\_log*

*sql\_tokens\_table=multiotp\_tokens*

*sql\_users\_table=multiotp\_users*

*syslog\_facility=7*

*syslog\_level=5*

*syslog\_port=514*

*syslog\_server=*

*tel\_default\_country\_code=*

*timezone=Europe/Zurich*

*token\_serial\_number\_length=12*

*token\_otp\_list\_of\_length=6*

*verbose\_log\_prefix=*

*# Run periodically:*

*./multiotp.php -debug -display-log -ldap-users-sync*

# Linux -työpöytien konfiguraatio

Linux-työpöydille on asennettu graafiseksi käyttöliittymäksi GNOME:

*sudo yum groupinstall -y "GNOME Desktop"*

Administrator required –ruutu on poistettu muokkaamalla */etc/xdg/autostart/gnome-software-service.desktop* –tiedostoa:

*# This will get rid of the admin pop-up on login  
X-GNOME-Autostart-enabled=false*

Käyttäjiä on estetty sulkemasta tai käynnistämättä palvelinta uudelleen muokkaamalla tiedostojen oikeuksia:

*chmod o-x /sbin/shutdown  
chmod o-x /sbin/reboot  
chmod o-x /sbin/halt  
chmod o-x /sbin/poweroff  
chmod o-x /bin/systemctl*

Pikakuvakkeiden luonti tapahtuu automaattisesti kirjautumisen yhteydessä, kun palvelimen */var/profile* –tiedostoon on lisätty seuraavat rivit:

*# Create shortcuts  
cp /usr/share/applications/desktopeditors.desktop /home/$USER/Desktop/desktopeditors.desktop  
cp /usr/share/applications/rstudio.desktop /home/$USER/Desktop/rstudio.desktop  
chmod u+x /home/$USER/Desktop/desktopeditors.desktop  
chmod u+x /home/$USER/Desktop/rstudio.desktop*

Käyttäjien asetuksista on (toistaiseksi manuaalisesti) estetty lukitusruutuun meneminen automaattisesti tietyn ajan jälkeen, koska lukitusruutu saattaa satunnaisesti jäätyä, jolloin käyttäjä ei pääse enää takaisin työpöydälle.

# SFTP -palvelin

Tiedostonsiirto ympäristöön tapahtuu SFTP-palvelimen kautta. Käyttäjä siirtää tiedostonsa SFTP-palvelimelle kertakäyttötunnuksella, mistä data siirtyy edelleen automaattisesti tiedostopalvelimella sijaitsevaan karanteeriin, josta ylläpitäjä käy siirtämässä sen asianmukaiseen hakemistoon. Tiedostonsiirtoa varten on pyydettävä palomuurilta portti 22 auki käyttäjän IP-osoitteesta SFTP -palvelimen IP -osoitteeseen. Lisäksi käyttäjälle on sallittava pääsy */etc/hosts.allow-*tiedostossa:

*# Nimi / Organisaatio*

*sshd: x.x.x.x : allow*

# Tekninen ympäristökuvaus

### Palvelinluettelo

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Palvelimin | DNS -nimi | IP osoite | Kuvaus | CPU | MEM | LEVY/ GB | Käyttöjärjestelmä |
| ISAACUSDC1 | ISAACUSDC1.ISAACUS.LOCAL | 193.166.16.140 | Domain Controller | 2 | 4 | C: 100 D: 100 | Windows 2016 |
| ISAACUSDC2 | ISAACUSDC2.ISAACUS.LOCAL | 193.166.16.141 | Domain Controller | 2 | 4 | C: 100 D: 100 | Windows 2016 |
| Isaacusipa1 | Isaacusipa1.ipa.isaacus.local | 193.166.16.142 | IPA Master | 2 | 4 | 100 | CentOS 7 |
| Isaacusipa2 | Isaacusipa2.ipa.isaacus.local | 193.166.16.143 | IPA Replica | 2 | 4 | 100 | CentOS 7 |
| ISAACUSCB1 | ISAACUSCB1.ISAACUS.LOCAL | 193.166.16.150 | RD Connection Broker | 2 | 4 | C: 100 | Windows 2016 |
| ISAACUSFS | ISAACUSFS.ISAACUS.LOCAL | 193.166.16.151 | Tiedostopalvelin (ylläpidon käyttöön) | 2 | 8 | C: 200 D: 256 | Windows 2016 |
| Isaacusbb | Isaacusbb.ipa.isaacus.local | 193.166.16.152 | Lokipalvelin | 2 | 4 | 100 | CentOS 7 |
| Isaacussw1 | Isaacussw1.ipa.isaacus.local | 193.166.16.153 | Spacewalk-palvelin | 2 | 4 | 100 | CentOS 7 |
| isaacusmfa | Isaacusmfa.isaacus.local | 193.166.16.154 | multiOTP-palvelin | 2 | 2 | 16 | CentOS 7 |
| ISAACUSADM | ISAACUSADM.ISAACUS.LOCAL | 193.166.16.160 | Windows-ylläpitopalvelin | 2 | 4 | C: 100 | Windows 2016 |
| Isaacusssh | Isaacusssh.ipa.isaacus.local | 193.166.16.161 | Linux-ylläpitopalvelin | 2 | 4 | 100 | CentOS 7 |
| Isaacusui | Isaacusui.ipa.isaacus.local | 193.166.16.170 | Edustapalvelin (Web) | 2 | 4 | 100 | CentOS 7 |
| Isaacusgm2 | Isaacusgm2.ipa.isaacus.local | 193.166.16.171 | Guacamole-palvelin | 2 | 4 | 100 | CentOS 7 |
| Isaacusrems | Isaacusrems.ipa.isaacus.local | 193.166.16.172 | REMS-palvelin | 2 | 4 | 100 | CentOS 7 |
| ISAACUSGW1 | ISAACUSGW1.ISAACUS.LOCAL | 193.166.16.173 | RD Gateway ja RD Web -palvelin | 2 | 2 | C: 100 | Windows 2016 |