TACACS+-HALLINNAN TOTEUTUS KESKI-SUOMEN SAIRAANHOITOPIIRIN VERKOSSA

Samppo Puranen

Opinnäytetyö
Marraskuu 2011

Tietotekniikka
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t) PURANEN, Samppo	Julkaisun laji Opinnäytetyö	Päivämäärä 10.11.2011
	Sivumäärä 57	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)

Työn nimi
TACACS+-HALLINNAN TOTEUTUS KESKI-SUOMEN SAIRAANHOITOPIIRIN VERKOSSA

Koulutusohjelma
Tietotekniikka

Työn ohjaaja(t)
NARIKKA, Jorma

Toimeksiantaja(t)
Jyväskylän Sähkötiimi Oy ja Keski-Suomen sairaanhoitopiirin lääkintätekniikka

Tiivistelmä

Opinnäytetyö tehtiin Jyväskylän Sähkötiimi Oy:lle ja Keski-Suomen sairaanhoitopiirin lääkintätekniikalle. Työssä selvitettiin mahdollisuutta ottaa Keski-Suomen sairaanhoitopiirin tietoverkossa käyttöön Cisco Systemsin Access Control System -palvelimet sekä niiden myötä TACACS+-, RADIUS- ja 802.1X -protokollat. Niiden lisäksi selvitettiin uusien toimintojen vaatimat muutokset kytkimien ja työasemien asetuksiin.

Opinnäytetyön tavoitteena oli tutkia mahdollisuutta luopua kytkimien yleisistä hallintatunnuksista ja ottaa käyttöön henkilöön sidotut hallintatunnukset. Muutokset tietoverkon toiminnallisuudessa oli testattava sekä luotava kirjallinen ohje lopulliseen käyttöön.

Selvitystyö tehtiin yhteistyössä sairaanhoitopiirin tietoverkkoinsinöörien kanssa. Toiminnallisuuden arviointi tapahtui kokeilemalla kytkimille kirjautumista, komentojen suorittamista, lokien tallentumista sekä mallinnettuja vikatilanteita. Koekäytössä hyödynnettiin samantyyppisiä verkkolaitteita kuin mitä on käytössä sairaanhoitopiirin tietoverkossa.

Työssä onnistuttiin Access Control System -palvelimien käyttöönotossa sekä verkkoprotokollien selvitystyössä. Työn tulokset otettiin osittain tuotantokäyttöön sairaanhoitopiirin tietoverkossa. Lääkintätekniikka kykenee dokumentaation avulla laajentamaan protokollien käyttöä tulevaisuudessa.

Avainsanat (asiasanat)
Tietoturva, pääsynvalvonta, TACACS+, RADIUS, 802.1X

Muut tiedot

Author(s)
PURANEN, Samppo

Type of publication
Bachelor´s Thesis

Date
10.11.2011

Pages
57

Language
Finnish

Confidential

( ) Until

Permission for web publication
(X)

Title
IMPLEMENTATION OF TACACS+ ADMINISTRATION IN THE CENTRAL FINLAND HEALTH CARE DISTRICT NETWORK

Degree Programme
Information Technology

Tutor(s)
NARIKKA, Jorma

Assigned by
Jyväskylän Sähkötiimi Oy and the Central Finland Health Care District

Abstract

The thesis was assigned by Jyväskylän Sähkötiimi Oy and the Central Finland Health Care District. The work explored the possibilities of deploying both Cisco Systems' Access Control System servers and TACACS+, RADIUS and 802.1X protocols in the Central Finland Health Care District network. In addition, the required changes to the switch configurations and workstation settings were studied.

The aim was to research the possibility to give up the use of the general administrator accounts and substitute them with person related administrator accounts. The changes in the network usability were to be tested and a document was to be produced for the actual deployment.

The study was carried out in cooperation with the network engineers of the Central Finland Health Care District. The evaluation of the functionality was made by logging in to the switches, running commands, checking log creation and by simulating errors. Similar networking equipment was utilized in the testing as the one that is in operational use in Health Care District network.

The assignment was successful in both the deployment of Access Control System servers and the study of networking protocols. The results have been deployed for partial use in the Central Finland Health Care District network. Health Care District's network engineers are able to expand the use of the networking protocols in the future with the help of the documentation produced.

Keywords
Information security, access control, TACACS+, RADIUS, 802.1X

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

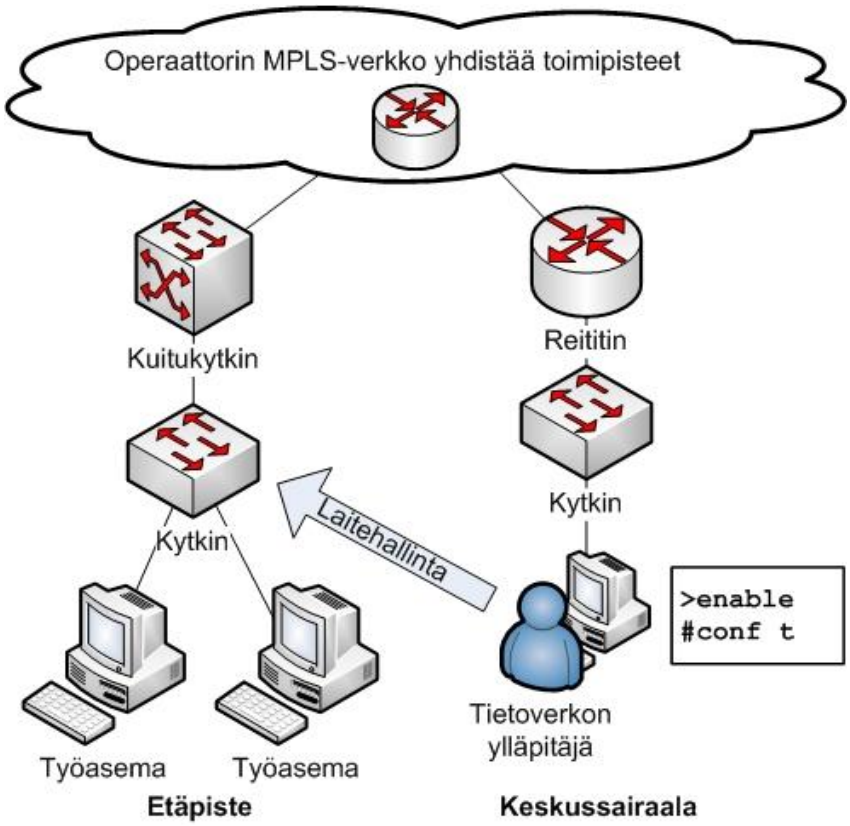
AAA	Authentication, Authorization and Accounting
ACS	Access Control System
AD	Active Directory
CLI	Command Line Interface
CSACS-1211	Cisco Systems Access Control System 1121
CSV	Comma Separated Value
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
MAB	MAC Authentication Bypass
MAC	Media Access Control
MD5	Message Digest Algorithm
MPLS	Multiprotocol Label Switching
MSCHAP v2	Microsoft Challenge Handshake Authentication Protocol version 2
NAD	Network Access Device
NDG	Network Device Group
NFS	Network File System
NTP	Network Time Protocol
OS	Operating System
PAE	Port Access Entity
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Access Dial In User Service
RFC	Request for Comments
SCP	Secure Copy Protocol

SFTP	SSH File Transfer Protocol
SSH	Secure Shell
TACACS+	Terminal Access Controller Acces-Control System Plus
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
VLAN	Virtual LAN
WWW	World Wide Web

1 OPINNÄYTETYÖN LÄHTÖKOHDAT

1.1 Lähtötilanne

Keski-Suomen sairaanhoitopiirin tietoverkkoa hallinnoivat Jyväskylän keskussairaalasta käsin lääkintätekniikkaosaston tietoverkkoinsinöörit. Heidän vastuullaan on muiden verkkolaitteiden ohella useita satoja kytkimiä, jotka välittävät tietoa ja muodostavat siten tietoverkon perustan. Suurin osa kytkimistä sijaitsee Jyväskylässä ja loput puolestaan eri puolilla Keski-Suomea. Kuviossa 1 on esitelty tietoverkon topologiaa.



KUVIO 1. Tietoverkko

Lääkintätekniikan tietoverkkoinsinöörit olivat tutustuneet aiemmin Cisco Systemsin ACS-palvelinteknologiaan. Sen perusteella lääkintätekniikka on päättänyt ottaa käyttöön kaksi ACS 5.2 -palvelinta ja niiden myötä TACACS+-protokollan. Muutoksella

tavoitellaan tietoverkon hallinnoimisen saattamista helposti skaalautuvaksi sekä edellytyksiä tietoverkon hallinnoinnin tietoturvan parantamiseen.

1.2 Tehtävä

Opinnäytetyö tehtiin Keski-Suomen sairaanhoitopiirin lääkintätekniikalle, joka osti työn Jyväskylän Sähkötiimi Oy:ltä. Jyväskylän Sähkötiimi Oy toimi työnantajana. Tehtävänä oli ottaa koekäyttöön ACS-palvelimet sekä TACACS+-protokolla, dokumentoida tulokset sekä lopulta ottaa tulokset osittain tuotantokäyttöön oikeassa käyttöympäristössä. Lopputuloksena syntyneen dokumentaation perusteella lääkintätekniikka kykenee laajentamaan TACACS+-protokollan käyttöön kaikille sairaanhoitopiirin kytkimille. Osa dokumentaatiosta rajattiin lääkintätekniikan käyttöön eikä ole siten julkista.

Opinnäytetyöhön ei sisältynyt erilaisten teknologioiden keskinäistä vertailua tai muita merkittäviä valintatehtäviä. Työstä rajattiin pois kytkinten ja työasemien asetusten tekeminen siltä osin, kuin ne eivät suoraan koskettaneet tavoiteltujen protokollien koekäyttöön ottamista.

Tavoitetilassa lääkintätekniikan tietoverkkoinsinöörit kirjautuvat kytkimille samoilla käyttäjätunnuksilla, kuin millä he kirjautuvat Windows-työasemillekin. Tällöin kirjautumistapahtuma on aina henkilöön sidottu. Jälkeenpäin on helppo tarkastaa, kuka kirjautui millekin kytkimelle ja mitkä komennot hän suoritti kytkimellä. Käyttäjätunnukset otetaan käyttöön ryhmäperusteisesti, jolloin käyttäjätunnusten hallinta on helposti skaalautuvissa. Käyttäjätunnukset liitetään haluttuihin ryhmiin, joiden mukaan tunnukset saavat eriasteisia oikeuksia kytkinten asetusten muokkaamiseen.

Opinnäytetyön käytännön osuuden ensimmäinen puolisko koostui CSACS-1211-palvelimen sekä TACACS+-protokollan käyttöönotosta koekäyttöön varatulla kytkimellä. Tämän jälkeen otettiin käyttöön toinen CSACS-1211-palvelin. Mikäli TACACS+-protokolla toimi, kokeiltiin myös 801.1X-todennuksen sekä RADIUS-protokollan käyttöönottoa TACACS+-protokollan rinnalle. Opinnäytetyön käytännön osuuden toinen

puolisko koostui toimivaksi saatujen protokollien kokeellisesta käyttöönotosta sairaanhoitopiirin kytkimissä. Samalla CSACS-1211-palvelimet päivitettiin viimeisimpään saatavilla olevaan versioon.

2 MUUTOKSET TIETOVERKON HALLINNASSA

2.1 Yleiset tavoitteet

Tietoverkon itsensä lisäksi sen hallinnan on hyvä olla tarvittaessa skaalautuva. Skaalautuvuus on mahdollista TACACS+-protokollan, Microsoft Corporationin AD-palvelimen sekä Cisco Systemsin ACS-palvelimen yhteistyönä. Yhteistyö toteutuu siten, että työntekijä kirjautuu kytkimelle samoilla AD-käyttäjätunnuksilla, kuin millä hän kirjautuu työasemansa Windows-käyttöjärjestelmään. Taustalla on henkilöön sidotun AD-käyttäjätunnuksen jäsenyys AD-käyttäjäryhmässä. Käyttäjäryhmä on puolestaan määritelty ACS-palvelimella osaksi säännön ehtoa, jonka perusteella kytkimelle saa tai ei saa kirjautua. Käyttäjätunnuksia koskeva tietoliikenne kytkinten sekä ACS-palvelimien välillä perustuu TACACS+-protokollaan. Tietoliikenne on salattua (User Guide for Cisco Secure Access Control System 5.3 2011, A-5).

Ryhmäjäsenyysperusteisella kirjautumisella saavutetaan monta etua. Kytkinten asetusten tekeminen on sidoksissa työntekijän henkilöllisyyteen. Työntekijän ei tarvitse muistaa kytkimille kirjautuessaan erillisiä kytkinten laitehallintaan varattuja hallintatunnuksia. Jos työntekijän työsuhde päättyy, häneltä tarvitsee sulkea vain yksi AD-käyttäjätunnus eikä hän pääse kirjautumaan sillä Windows-työasemille tai kytkimille. Tietoverkon ylläpitäjien ei tarvitse vaihtaa hallintatunnuksia kuin harvoin, ja käyttäjätunnuksista vastaavien on nopeaa lisätä tarvittavat käyttäjätunnukset oikeisiin käyttäjäryhmiin. Vanhassa mallissa kytkinten hallintatunnus oli yhteinen ja siten erillinen työntekijöiden omista Windows-käyttäjätunnuksista.

Mikäli jostain syystä kytkinten laitehallinnassa ei voida tai ei haluta tukeutua AD-pohjaiseen ryhmäjäsenyyteen, on mahdollista luoda hallintatunnukset ja käyttäjäryhmät suoraan ACS-palvelimelle. Tämä antaa pelivaraa toteutuksen suhteen. ACS-palvelimelle luotuja hallintatunnuksia voidaan tarvittaessa antaa luotettujen sairaanhoitopiirin ulkopuolisten asiantuntijoiden käyttöön. Tällaisia erityistarpeita varten voidaan luoda rajoitukset laite- ja komentotasoilla.

Siltä varalta, että AD- ja ACS-palvelimet ovat kummatkin poissa käytöstä, kytkimille on aina mahdollista kirjautua paikallisella kytkimelle asetetulla enable-salasanalla. Tällä tavalla kokonaisuus ei ole ACS-palvelimien toiminnasta riippuvainen. Periaatteessa kaikkien tietoverkon ylläpitäjien ei tarvitse edes tietää enable-salasanaa.

Mikäli 802.1X-todennus saadaan toimimaan tietoverkossa, kytkin yrittää todentaa työasemat ja muut siihen kytketyt tietotekniset laitteet AD-palvelimelta ja luo sen perusteella lokimerkinnän. 802.1X on avoimessa tilassa, jolloin kaikki pääsevät kytkeytymään tietoverkkoon. Syntyneitä lokimerkintöjä voidaan käyttää myöhemmin apuna päätöksenteossa, kun pohditaan tietoverkkoon kytkeytymisen rajoittamista 802.1X-todennuksen avulla.

2.2 Authentication, Authorization and Accounting

Authentication, Authorization and Accounting on tietoturvaprotokolla, joka on suomeksi todennus, valtuutus ja tilastointi. Todennuksella varmistetaan henkilöllisyys, valtuutuksella tarkistetaan toimintaoikeudet ja tilastoinnilla pidetään kirjaa tapahtumista myöhempää seurantaa varten. Kaikki kolme ovat tärkeitä työntekijöiden henkilökohtaisen vastuun kannalta. AAA-toteutuksen avulla on mahdollista tarvittaessa jälkikäteen osoittaa, että joku tietty työntekijä on tai ei ole voinut aiheuttaa tapahtunutta muutosta tietoverkon toiminnassa.

Tavoitetilassa AAA-protokollaa noudatetaan kytkinten laitehallinnassa siten, että todennuksessa työntekijän henkilöllisyys varmistetaan AD- ja ACS-palvelimien tietokannoista. Valtuutus toteutuu siten, että ACS-palvelimelle asetetuilla säännöillä salli-

taan ja estetään komentojen suorittaminen kytkimillä. Tilastoinnissa ACS-palvelin kerää lokia kytkimillä suoritetuista komennoista.

2.3 Kytkinten laitehallinta

Kytkinten laitehallinnan kannalta kytkinten on vaadittava sisäänkirjautuminen, ennen kuin käyttäjä voi muuttaa kytkinten asetuksia tai katsella niiden tietoja. Kytkimen tulee hyväksyä sekä AD- että ACS-palvelimelle luodut sääntöjen mukaiset käyttäjätunnukset. Lisäksi kytkimillä on oltava paikalliset enable-salasanat, joihin tukeudutaan silloin, kun yhteydet ACS- ja AD-palvelimiin eivät toimi tai ole käytössä. Lopuksi kytkinten on noudatettava käyttäjälle asetettuja komentorajoituksia sekä lähetettävä tiedot suoritetuista komennoista ACS-palvelimelle lokimerkinnöiksi.

3 TERMINAL ACCESS CONTROLLER ACCESS-CONTROL SYSTEM PLUS

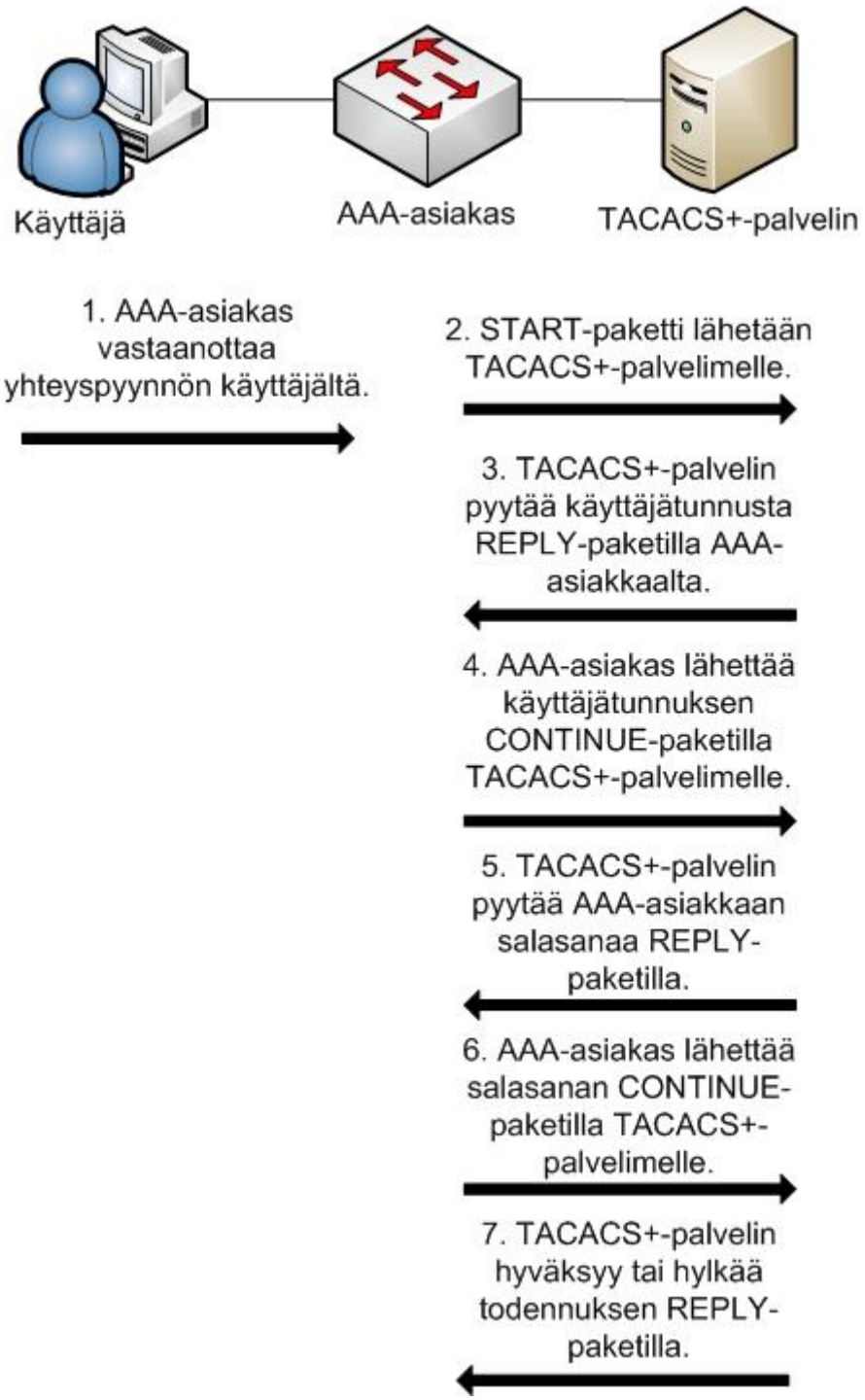
Terminal Access Controller Access-Control System Plus -protokolla on Cisco Systemsin kehittämä protokolla, joka perustuu aiempaan TACACS-protokollaan (Santuka, Banga & Carroll 2011, 13). TACACS+-protokolla mahdollistaa käyttäjän todennuksen, valtuutuksen sekä tilastoinnin ja siten muodostaa yhden AAA-protokollan toteutuksen mahdollisista työkaluista.

TACACS+-protokollaa hyödyntävä järjestelmä koostuu kolmesta osasta: käyttäjästä sekä hänen työasemastaan, AAA-asiakkaasta kuten kytkimestä tai reittitimestä sekä TACACS+-palvelimesta, jota kutsutaan myös AAA-palvelimeksi. Toimiva TACACS+-protokollan käyttöönotto vaatii asetusten teot AAA-asiakkaalle ja AAA-palvelimelle.

Viestiliikenne AAA-asiakkaan sekä TACACS+-palvelimen välillä kulkee TCP-protokollan määrittämässä muodossa portista 49. TACACS+-paketit voivat olla joko todennus-, valtuutus- tai tilastointipaketteja. Kumpaankin päähän on asetettava sama jaettu

salausavain, jonka tiiviste on luotu MD5-algoritmilla (Santuka ym. 2011, 15). Salausavainta ei siirretä tietoverkon kautta (Sankar, Sundaralingam, Balinsky & Miller 2005, 44).

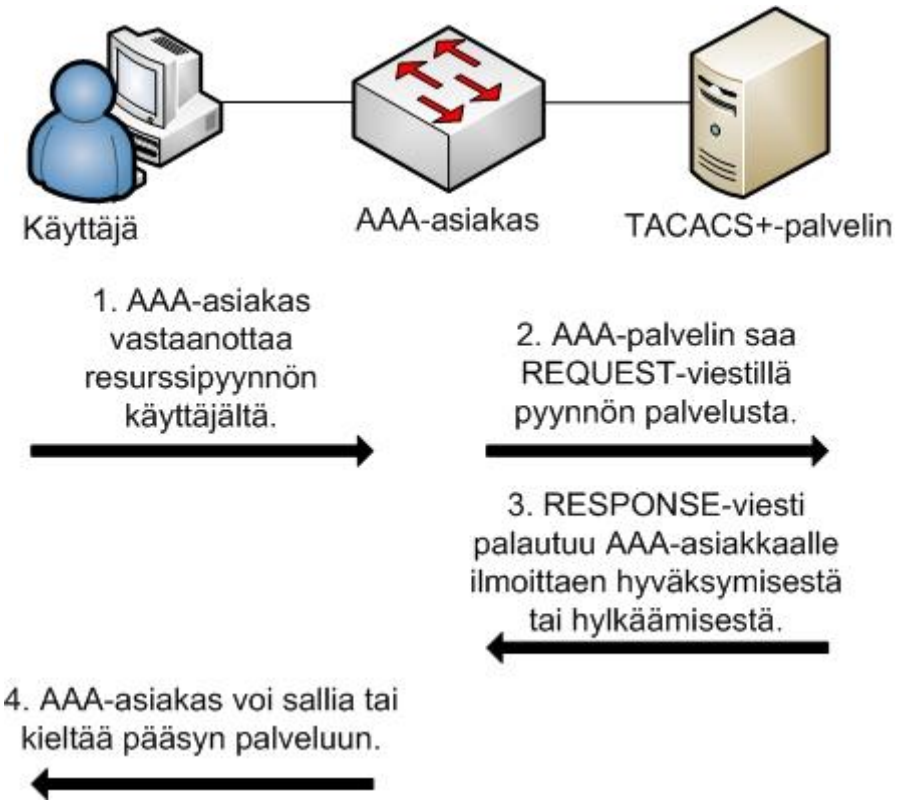
TACACS+-todennuksessa AAA-asiakas voi lähettää AAA-palvelimelle START- ja CONTINUE-viestit. START aloittaa viestinnän, ja CONTINUE välittää käyttäjäntunnuksen sekä salasanan. AAA-palvelimen REPLY-vastaus voi sisältää seuraavat arvot: ACCEPT, REJECT, ERROR tai CONTINUE. ACCEPT hyväksyy todennuksen, REJECT hylkää todennuksen, ERROR ilmoittaa virheestä ja CONTINUE pyytää lisätietoja. Esimerkki todennuksesta näkyy kuviossa 2. (Santuka ym. 2011, 16-17.)



KUVIO 2. TACACS+-todennus (Santuka ym. 2011, 16)

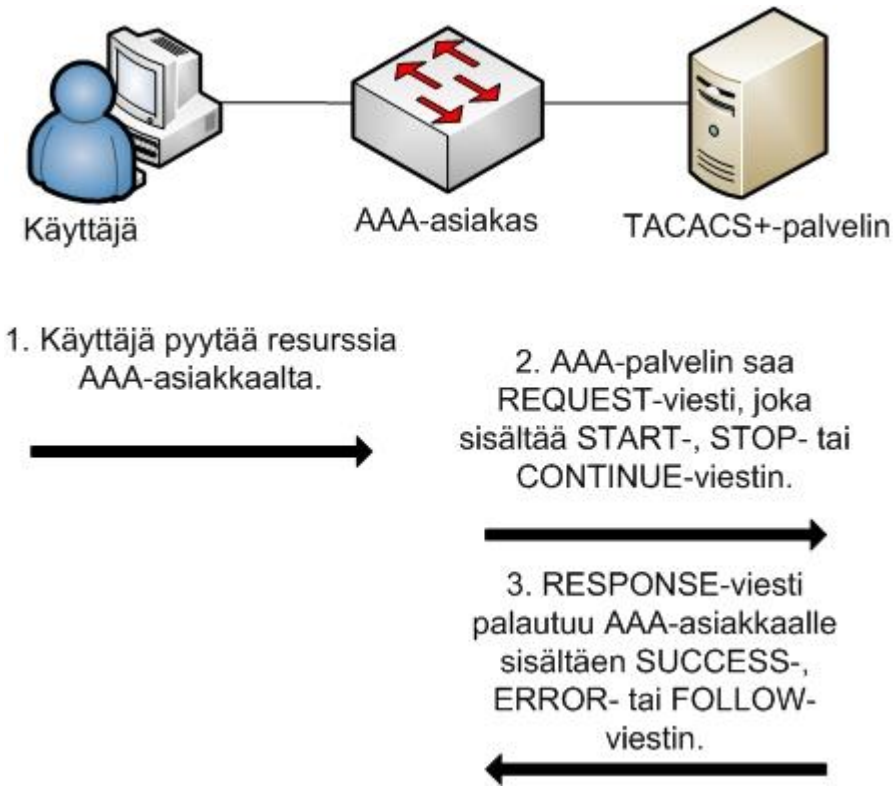
Valtuutuksessa kulkevat REQUEST- ja RESPONSE-viestit. Santukan ja muiden (2011) esimerkkiä mukaileva TACACS+-valtuutus näkyy kuviossa 3. Kielteisessä valtuutustapauksessa komentoliittymään tulee Command authorization failed -ilmoitus. Komentojen valtuutuksen käyttöönoton myötä on mahdollista, että käyttäjä kirjautuu sisälle

kytkimelle tai reittittimelle ilman, että hänellä on kuitenkaan oikeuksia suorittaa yhtäkään komentoa.



KUVIO 3. TACACS+-valtuutus (Santuka ym. 2011, 18)

Tilastoinnissa kulkevat REQUEST -ja RESPONSE-viestit, joista jälkimmäinen voi sisältää SUCCESS-, ERROR- tai FOLLOW-tiedon. RESPONSE-viestit ovat AAA-palvelimen vastauksia AAA-asiakkalle. SUCCESS kertoo AAA-palvelimen vastaanottaneen onnistuneesti tilastointitiedot, ERROR kertoo AAA-palvelimen epäonnistuneen tilastointitiedon syöttämisessä tietokantaansa ja FOLLOW ohjeistaa AAA-asiakkaan lähettämään tiedot toiselle AAA-palvelimelle (Santuka ym. 2011, 19). Kuviossa 4 näkyy esimerkki viestiliikenteestä.



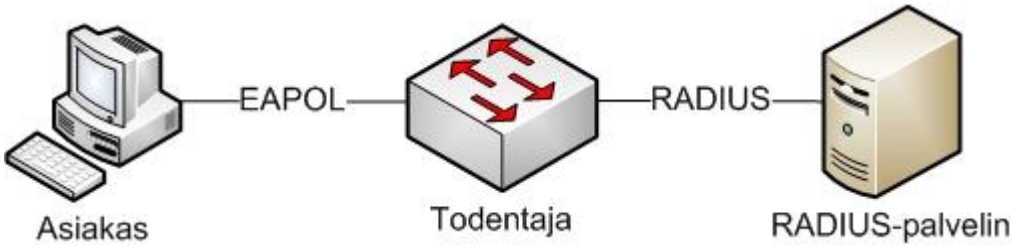
KUVIO 4. TACACS+-tilastointi (Santuka ym. 2011, 20)

4 802.1X-TODENNUS JA RADIUS

4.1 Käyttö

802.1X-todennus mahdollistaa porttikohtaisen todennuksen, jonka avulla verkkolaiteita ei päästetä tietoverkkoon ennen niiden todentamista tietokannoista. 802.1X-todennuksen toteutus käsittää asiakkaan, todentajan ja todennuspalvelimen. Toimiva 802.1X-toteutus vaatii tuen kaikilta kolmelta osapuolelta. Asiakas on työasema, todentaja on joko kytkin, reititin tai langattoman tietoverkon tukipiste ja todennuspalvelin on RADIUS-palvelin.

802.1X-todennuksessa aloite voi olla joko asiakkaalla tai todentajalla tilanteesta riippuen. Asiakas, todentaja ja RADIUS-palvelin vaihtavat tietoja EAPOL-kapseloidulla EAP-viesteillä ja RADIUS-protokollan mukaisilla viesteillä. Menetelmä riippuu kuvion 5 mukaisesti siitä, minkä laitteiden välinen tiedonsiirto on kyseessä.



KUVIO 5. EAPOL ja RADIUS

EAP on asiakirjassa RFC 3748 määritelty protokolla, jota käytetään asiakkaan ja todennuspalvelimen välillä (Aboba, Blunk, Vollbrecht, Carlson, & Levkowetz 2004). EAP toimii puitteena, ja sen sisällä käytettäviä todennusmenetelmiä ovat muun muassa EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, PEAP, LEAP sekä EAP-TTLS. EAP kapsuloidaan tietoliikennettä varten EAPOL-protokollalla. (Santuka ym. 2011, 197-199.)

RADIUS on TACACS+-protokollan ohella toinen yleinen AAA-protokolla. RADIUS tukee todentamista, valtuutusta ja tilastointia, joista kaksi ensimmäistä RADIUS yhdistää yhdeksi kokonaisuudeksi. Toisin kuin TACACS+, RADIUS-protokolla salaa tietoliikenteestään ainoastaan salasanan, mutta ei muuta. Tiedonsiirto tapahtuu UDP-porteilla 1645, 1812, 1646 ja 1813. (Santuka ym. 2011, 9-11.)

Todentajilla on mahdollista asettaa, voiko samaan porttiin kytkeytyä yksi vai useampi asiakas. Vaihtoehdot ovat single-host mode, multiple-host mode, multidomain authentication mode ja multiauthentication mode. Single-host mode sallii vain yhden asiakkaan porttia kohden. Multiple-host mode sallii usean asiakkaan kytkeytyä samaan porttiin, mikäli ensimmäinen asiakas todennettiin. Multidomain authentication mode sallii kahden tietoliikennettä tai ääniliikennettä hyödyntävän laitteen toisistaan erilliset todennukset ja VLAN-verkot samassa portissa. Multiauthentication mode sallii yhden asiakkaan ääniliikenteelle varattuun VLAN-verkkoon ja useita asiakkaita tietoliikenteelle varattuun VLAN-verkkoon. (Santuka ym. 2011, 206-208.)

Edellisessä kappaleessa lueteltujen neljän vaihtoehdon lisäksi voidaan samanaikaisesti käyttää open mode -tilaa, jolloin kaikki liikenne sallitaan todennuksesta riippumatta (Tägström 2011, 15). Täten 802.1X-protokollan toimivuutta voidaan kokeilla

ilman käyttökatkoksia. Verkkoliikenteestä RADIUS-palvelimelle syntynyt lokitieto auttaa päätöksenteossa siinä tilanteessa, kun pohditaan 802.1X-todennusta verkkoonpääsyn ehdoksi. Open mode -tila asetetaan kytkimillä porttikohtaisesti authentication open -komennolla.

4.2 802.1X-yhteensopimattomat laitteet

802.1X-yhteensopimattomia laitteita ovat tyypillisesti verkkotulostimet, faksit, UPS-laitteet ynnä muut vastaavat. Verkkotulostimien 802.1X-yhteensopivuus vaihtelee malleittain. 802.1X-yhteensopimattomia laitteita varten on olemassa MAC-osoitteeseen perustuva MAC Authentication Bypass -todennusmenetelmä. MAB-yhteydenotto tunnetaan myös host lookup request -nimellä (User Guide for Cisco Secure Access Control System 5.3 2011, 3-7).

MAB-menetelmä perustuu RADIUS-palvelimella sijaitsevaan tietokantaan, joka sisältää verkkotulostimien ja muiden verkkolaitteiden MAC-osoitteet. Jos MAC-osoite löytyy tietokannasta, RADIUS-palvelin palauttaa kytkimelle ilmoituksen onnistuneesta MAB-kyselystä. Sen tuloksena kytkin avaa tarvittavan portin (Introduction to IEEE 802.1X and Cisco® Identity-Based Networking Services (IBNS) 2008, 29).

5 ACS-PALVELIN

5.1 Yleistä

Cisco Systemsin valmistama Cisco 1121 Access Control System on kooltaan standardin mukainen laiteräkkiin asennettava 1U-palvelin. Palvelimet asennetaan tyypillisesti konesaliin tai laitekaappiin. CSACS-1121 on varustettu Intelin 2,66 GHz:n neliydinprosessorilla ja kahdella 250 gigatavun kovalevyllä (Cisco Secure Access Control System 5.3 2011, 3). Käyttöjärjestelmänä toimiva Cisco Application Deployment Engine

OS 1.2 on Linux-pohjainen (User Guide for the Cisco Secure Access Control System 5.3 2011, 1-2).

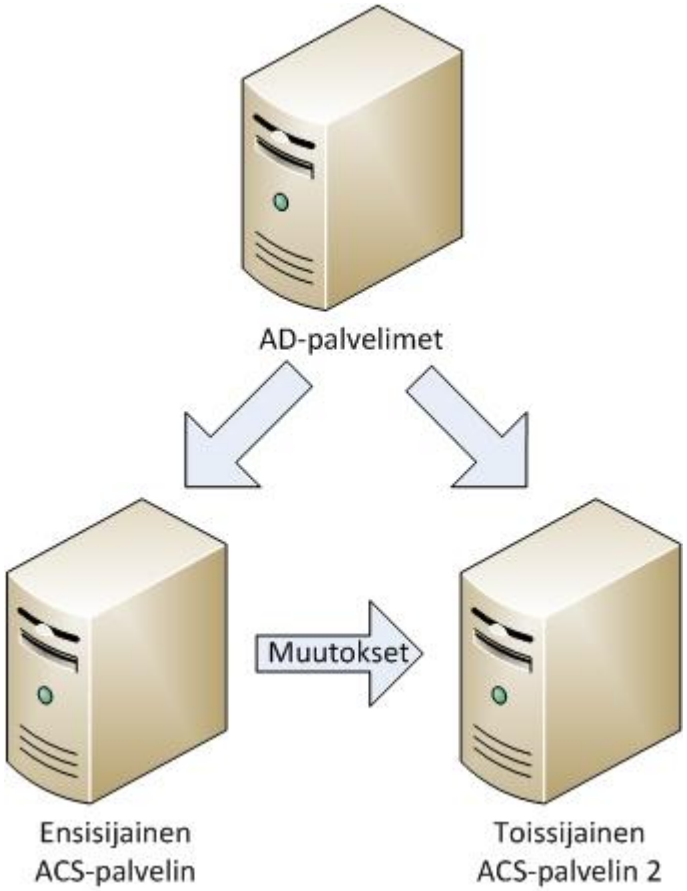
ACS-palvelimen tehtävä on tehostaa tietoverkon turvallisuutta toimimalla sekä TACACS+- että RADIUS-palvelimena. Lisäksi ACS-palvelin kykenee pitämään kirjaa tietoverkkolaitteilla ajetuista komennoista. Nämä ACS-toiminnot koskettavat vain niitä verkkolaitteita, joiden tiedot on lisätty ACS-palvelimen tietokantaan.

Kirjoitushetkellä viimeisin ACS-palvelimen ohjelmiston versio on 5.3, jonka oletuslisenssi Base License sallii 500 verkkolaitteen hallinnan. Mittarina toimivat verkkolaitteiden yksilölliset IP-osoitteet. Tarvittaessa määrän ylärajaa voidaan nostaa ostamalla Cisco Systemsiltä Large Deployment Add-On License -lisenssi. Jos useita ACS-palvelimia yhdistetään keskenään yhdessä toimivaksi ACS-palvelinryhmäksi, on niillä silti vain yhden lisenssin verran käytettävissä verkkolaitteiden rekisteröintitilaa. Tämä johtuu siitä, että verkkolaitetiedot kopioituvat ACS-palvelinryhmässä palvelimelta toiselle.

ACS-palvelimien hallinta tapahtuu graafisella GUI-käyttöliittymällä, johon päästään ottamalla Internet-selaimella turvallinen HTTPS-yhteys ACS-palvelimen IP-osoitteeseen. Rajoitetumpi määrä toimintoja voidaan tehdä ottamalla ACS-palvelimeen turvallinen SSH-yhteys. Vaihtoehtoisesti ACS-palvelimeen voidaan ottaa konsoliyhteys paikan päällä konesalissa. SSH- tai konsoliyhteydellä ACS-palvelinta hallitaan tekstipohjaisella CLI-käyttäliittymällä.

5.2 Usean ACS-palvelimen yhteistoiminta

Samassa tietoverkossa voi olla useampi kuin yksi ACS-palvelin käytössä, jolloin ne jaetaan ensisijaisiksi sekä toissijaisiksi ACS-palvelimiksi. Käytössä on aina yksi ensisijainen ACS-palvelin, ja loput ovat toissijaisia palvelimia. Ensisijaisella palvelimella tehtävät asetukset kopioituvat toissijaisille palvelimille kuvion 6 mukaisesti. Toissijaiset ACS-palvelimet eivät keskustele keskenään, mutta kykenevät ottamaan omatoimisesti yhteyden AD-palvelimiin todennusta varten.



KUVIO 6. Usean ACS-palvelimen yhteistoiminta

Kahden ACS-palvelimen toimintamallilla saavutettaviin etuihin kuuluu kahdentamisesta syntyvä redundanttisuus, joka antaa lisäturvaa laiterikon varalta. Toisena etuna kaikki valvontaan liittyvät kirjautumiset voidaan tehdä tietoverkon valvontaan varatulle Monitoring & Report Viewer -palvelimelle, mikä on myös valmistajan suositus (User Guide for the Cisco Secure Access Control System 5.3 2011, 19-2). Kolmantena etuna todennuksesta, valtuutuksesta ja tilastoinnista syntyvää tietoliikennettä voidaan tarvittaessa jakaa ACS-palvelinten kesken. Käytännössä viimeksimainittu tehdään asettamalla kytkimille eri ACS-palvelimet järjestyksessä ensisijaisiksi.

Toissijaiselle ACS-palvelimelle on mahdollista tehdä tarvittaessa tilapäisiä paikallisia asetuksia. Roolienvaihdot ensisijaisen ja toissijaisen ACS-palvelimen välillä ovat myös mahdollista. Tällaiset poikkeukset voivat tulla kyseeseen laiterikon kohdalla.

5.3 Laitehallinnan toimintaperiaate

Tietoverkon ylläpitäjät lisäävät hallinnoitavien kytkinten tiedot ensisijaisen ACS-palvelimen laitetietokantaan. Lisäyksen yhteydessä määritellään kytkimelle nimi, kuvaus, jäsenyys halutuissa sijainti- ja laitetyyppiryhmissä, IP-osoite sekä käytettävä todennusprotokolla.

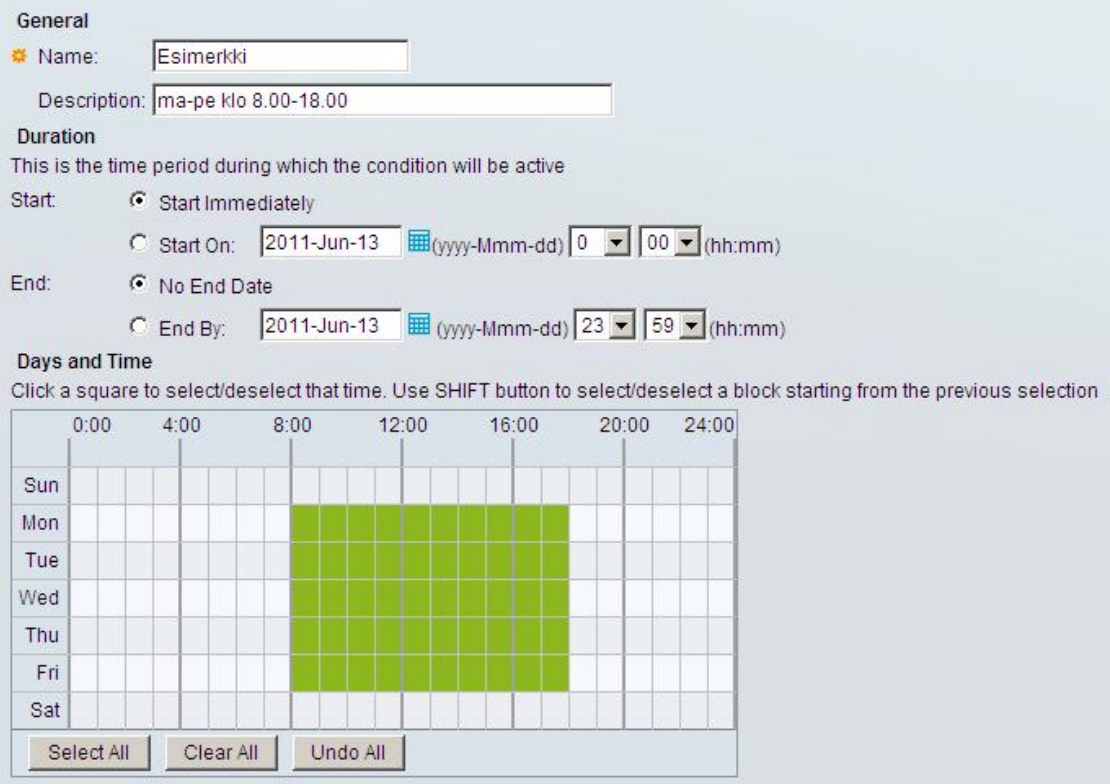
Sijainti- ja laitetyyppiryhmiä on kumpiakin mahdollista luoda tarpeen mukaan. Sijainti voi olla esimerkiksi paikkakuntaperusteinen tai rakennusperusteinen. Laitetyyppiryhmät voidaan puolestaan jakaa vaikkapa tyypin, valmistajan tai mallin mukaan. Ryhmiä kutsutaan Network Device Group -ryhmiksi ja ne voidaan järjestellä hierarkiaan. Kuviossa 7 näkyy esimerkki paikkaperusteisesta NDG-ryhmästä, joka on ryhmän All Locations aliryhmä.

KUVIO 7. Network Device Group

IP-osoite voidaan asettaa joko yksittäisenä osoitteena tai IP-osoitejoukkona. Yhdelle laitteelle voidaan asettaa korkeintaan 40 IP-osoitetta (User Guide for the Cisco Secure Access Control System 5.3 2011, 7-11). Todennusprotokolla voi olla TACACS+, RADIUS tai kumpikin. Kummallekin protokollalle täytyy asettaa jaettu salausavain.
Kun hallinnoitavien verkkolaitteiden tiedot on syötetty ACS-palvelimelle, voidaan luoda säännöstö, jonka mukaan laitehallinta toteutuu. Ensisijaisella ACS-palvelimella voidaan määritellä protokollien yksityiskohtaiset asetukset, henkilöllisyystietokannat, aikataulut sekä laitteilla suoritettavien komentojen luvallisuus.

Henkilöllisyystietokantoja voi olla useita ja niiden läpikäyntijärjestys on valittavissa. Eri tarpeita varten voidaan luoda omat läpikäyntijärjestyksensä. Esimerkiksi on mahdollista verrata kytkimelle syötettyjä hallintatunnuksia sekä AD-palvelimen käyttäjätunnuksiin että myös ACS-palvelimelle luotuihin hallintatunnuksiin.

Aikatauluja voi olla olemassa useita samanaikaisesti ja niille voidaan asettaa alkamis- sekä loppumisajankohdat. Kellonaikojen valinta tapahtuu kuvion 8 mukaisesti.

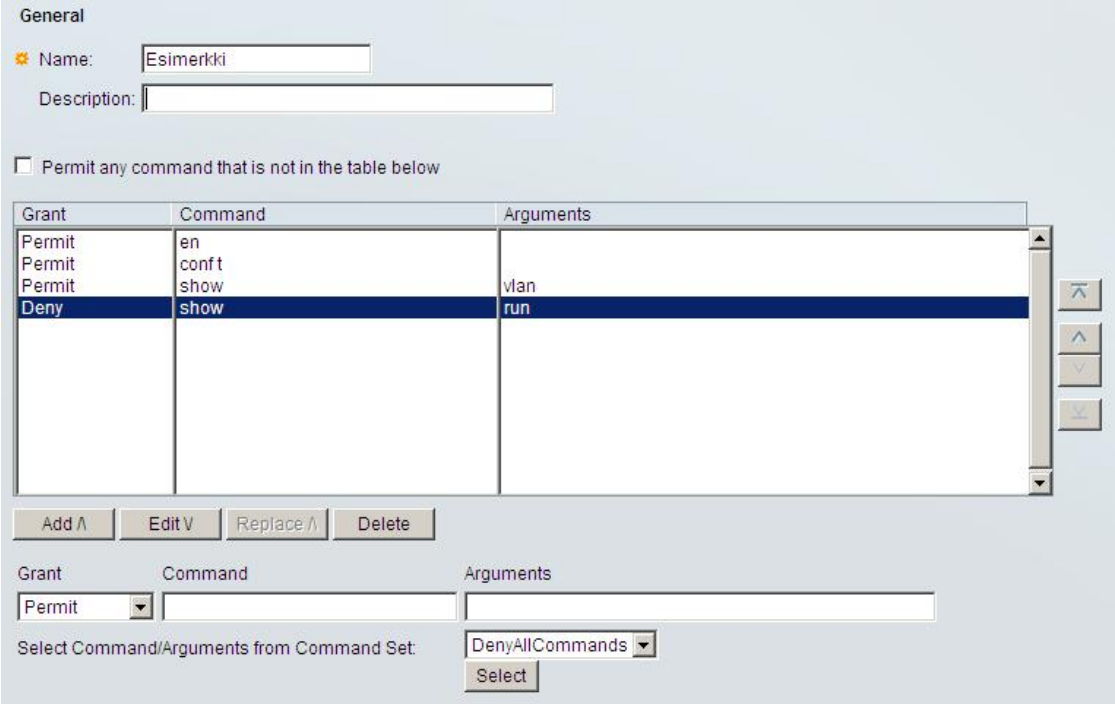


KUVIO 8. Esimerkki viikkoaikataulusta

Komentojen lupatarkistus voidaan toteuttaa käyttäen joko command sets tai shell profiles -ominaisuuksia (User Guide for the Cisco Secure Access Control System 5.3 2011, 9-23). Kummallakin on mahdollista toteuttaa jako kahteen eritasoiseen hallintaoikeuteen. Tällöin on olemassa erikseen sekä lukuoikeus kytkinten asetusten katsomiseen että myös luku- ja kirjoitusoikeus asetusten muuttamiseen. Tällaisellä jaottelulla toteutetaan pienimmän tarvittavan oikeuden periaatetta. ACS-palvelimen

käyttöjärjestelmä sallii tai kieltää verkkolaitteilta komentojen suorittamisen ja välittää tiedon takaisin kytkimille.

Cisco Systemsin kytkimissä käyttäjien oikeudet määrää privilege level -taso. Alin taso on 0 ja vastaavasti korkein taso on 15, jota kutsutaan enable-tilaksi. Kun käyttäjä kirjautuu kytkimelle, privilege level on oletuksena 0. Privilege level -tason määrityksen lisäksi komentoja voidaan erikseen tai implisiittisesti kieltää ja sallia kuvion 9 mukaisesti.



KUVIO 9. Command Set

Jokaista tarvetta kohden luodaan oma palvelunsa. Esimerkiksi voidaan luoda palvelu, että TACACS+-protokollaa hyödyntäen tietyssä AD-käyttäjäryhmässä olevat käyttäjät pääsevät suorittamaan privilege level 15 -tasoisia komentoja tietyillä kytkimillä. Palvelut kootaan listaksi, johon ACS-palvelin vertaa tilanteita järjestyksessä ylhäältä alas. Näiden lisäksi on olemassa oletussääntö, johon ACS-palvelin tukeutuu, mikäli tilanne ei vastaa yhtään palvelua. Taulukossa 1 näkyy esimerkki ACS-palvelimen palveluiden

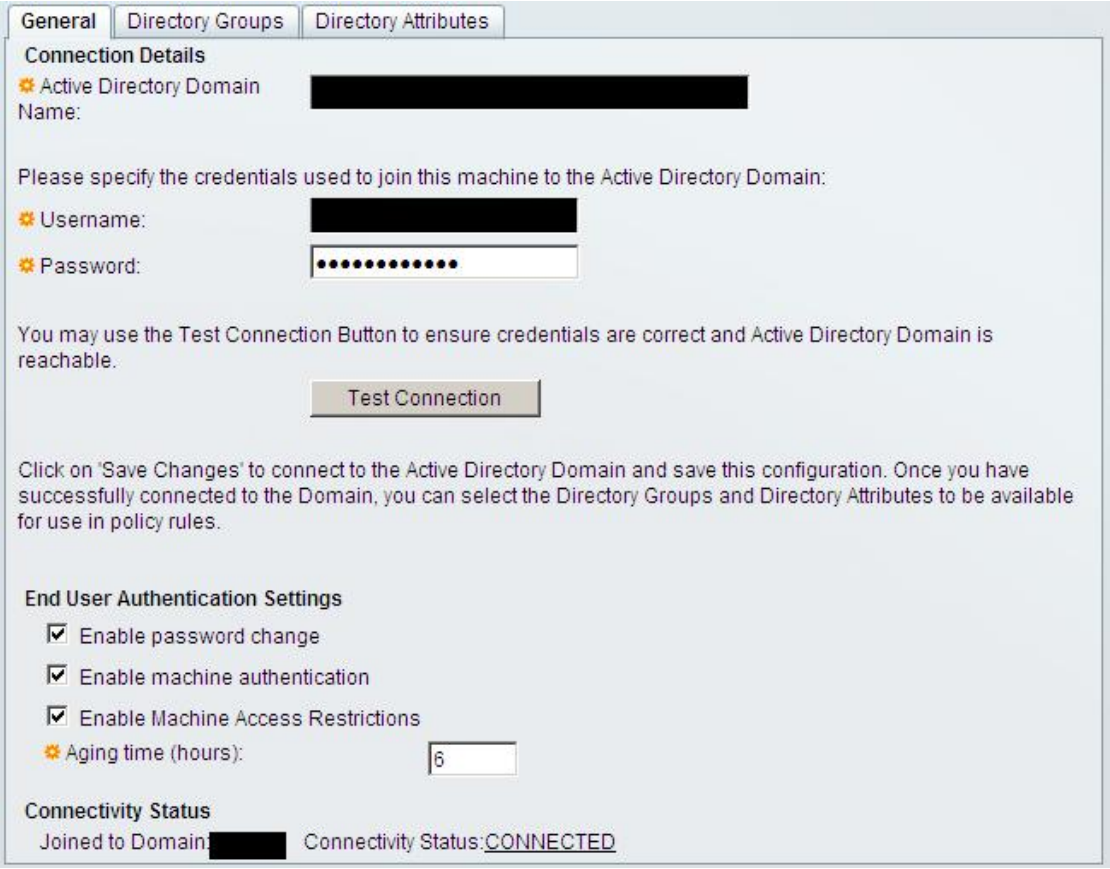
eri tarkoituksista, ehdoista ja laitetietokannoista. Taulukon esimerkistä on jätetty pois oikeassa käytössä tärkeitä yksityiskohtia.

TAULUKKO 1. ACS-palvelimen palveluita

Käyttötarkoitus	Ehdot	Laitetietokanta
langaton MAC-pohjainen laitetodennus	match Radius, match Host Lookup	internal hosts
MAC-pohjainen laiteto-dennus	match Radius, match Host Lookup	internal hosts
työaseman langaton 802.1X-todennus	match Radius	AD
työaseman 802.1X-todennus	match Radius	AD
yhteistoiminta WCS:n kanssa	match Tacacs	NDG
kytkinten laitehallinta	match Tacacs	NDG

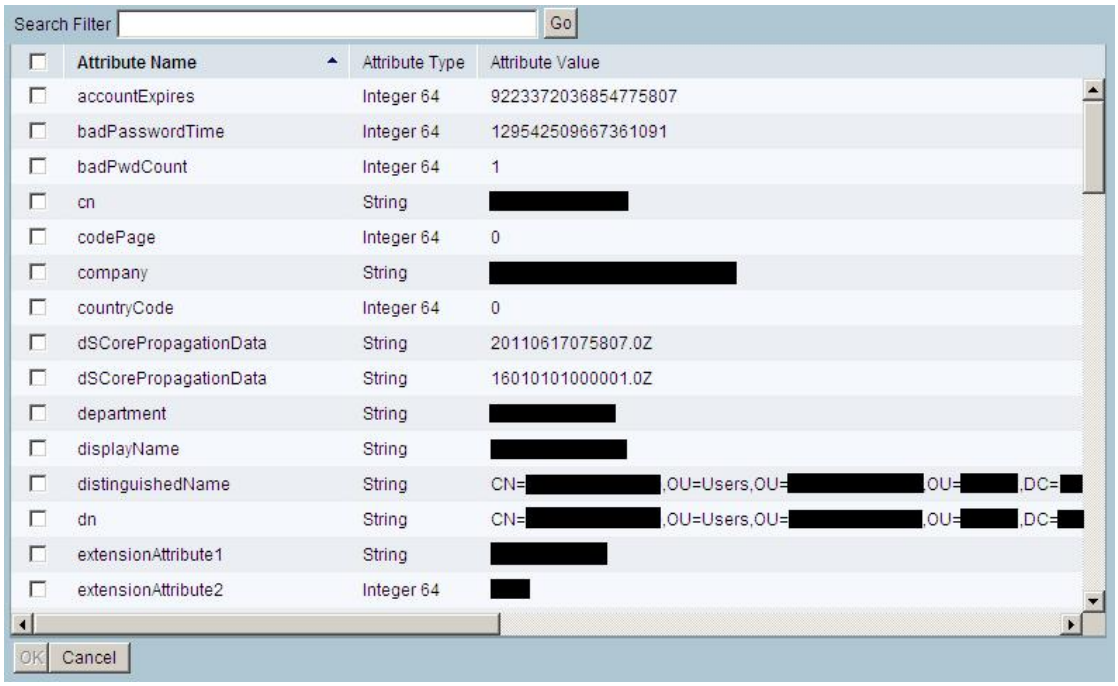
5.4 Yhteistyö AD:n kanssa

Aikaisemmin mainittujen ACS- ja AD-palvelimien yhteistyöllä saatavien etujen lisäksi kytkimelle kirjautuminen ei onnistu, jos AD-pohjainen käyttäjätunnus on lukossa, vanhentunut tai suljettu (User Guide for Cisco Secure Access Control System 5.3 2011, 8-41). Tätä varten ACS-palvelin luo IdentityAccessRestricted-ehdon, jota voidaan käyttää sääntöjen osana. Kuviossa 10 näkyy ACS-palvelimen sivu, jossa palvelin liitetään AD-toimialueeseen. Ikkunaan syötettävällä käyttäjätunnuksella on oltava riittävät valtuudet AD-todennuksia varten, joten se ei saa vanhentua tai muuten yhteys ACS- ja AD-palvelimien välillä katkeaa.



KUVIO 10. AD-yhteys

AD-toimialueesta on mahdollista poimia halutut ryhmät käytettäviksi sääntöjen ehtoina. Niin toimittaessa käyttäjätunnusten hallintatoimet tarvitsee tehdä vain AD-palvelimella. Kuviossa 11 näkyy käyttäjätunnuksien ominaisuuksia, joita voidaan poimia sääntöjen ehdoiksi. Samalla toiminnolla on mahdollista tutkia työasemien tietoja. Tällöin työaseman tiedot syötetään muodossa host/isäntänimi, siinä missä käyttäjätunnukset syötetään sellaisenaan.

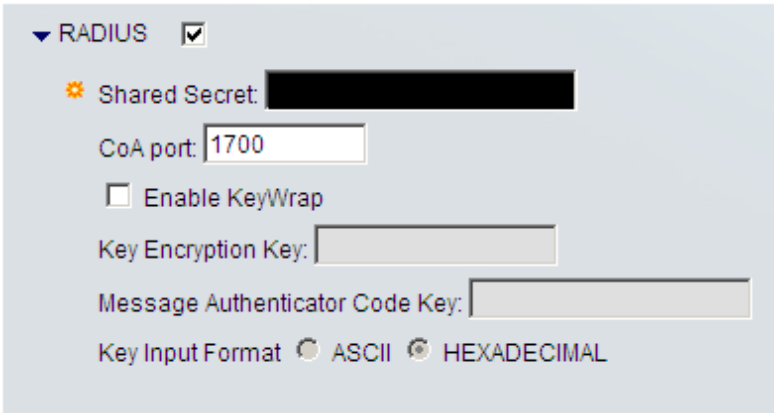


KUVIO 11. Directory Attributes

AD- ja ACS-palvelimien tulee olla synkronisoituja Network Time Protocol -palvelimen ajan mukaisesti. Palvelimien on haettava aika samalta NTP-palvelimelta. Aikaero voi aiheuttaa ongelmia toiminnan kannalta. (User Guide for Cisco Secure Access Control System 5.3 2011, 8-39.)

5.5 ACS-palvelin, 802.1X ja RADIUS

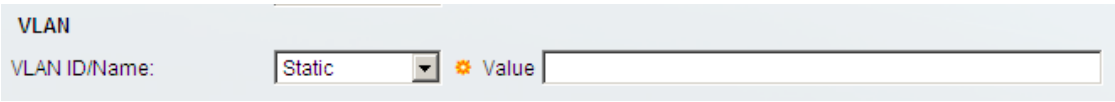
ACS-palvelin voi toimia RADIUS-palvelimena 802.1X-todennusta varten. Kytkimille on asetettava ACS-palvelinten IP-osoitteet ja ACS-palvelimella laitetaan rasti ruutuun Network Devices and AAA Clients -asetuksissa kuvion 12 mukaisesti sekä lisätään salausavain.



KUVIO 12. RADIUS-asetukset

ACS-palvelimelle tulee asettaa Internal Host -kohtaan MAC-osoitteet sellaisista 802.1X-todennusta tukemattomista verkkolaitteista, jonka halutaan pääsevän tieto-verkkoon. Koska MAC-osoitteita voi olla tuhansia tai kymmeniä tuhansia, tiedot on mahdollista tuoda ACS-palvelimelle csv-tietokantana (User Guide for Cisco Secure Access Control System 5.3 2011, 7-8).

ACS-palvelin voi palauttaa kytkimelle tiedon VLAN-verkosta, johon portti asetetaan. Asetus tehdään valitun Authorization Profile -mallin Common Tasks -välilehdellä kuvion 13 mukaisesti.



KUVIO 13. VLAN

802.1X-yhteensopivat Windows-työasemat voidaan todentaa AD-palvelimilta (User Guide for Cisco Secure Access Control System 5.3 2011, B-34-B-35). Työaseman isäntänimeä verrataan AD-palvelimen tietokantaan. Konetodennuksessa ACS-palvelin toimii välikätenä todentajan ja AD-palvelimien välillä.

5.6 Sisäiset hallintatunnukset

ACS-palvelimelle voidaan luoda sisäisiä hallintatunnuksia AD-palvelimella sijaitsevien ulkoisten käyttäjätunnusten lisäksi. Hallintatunnukset luodaan Internal Indetity Stores -valikossa Internal Users -nimikkeellä. Hallintatunnuksille on mahdollista asettaa jäsenyys halutussa identiteettiryhmässä, mikä sekin voi olla ehtona säännöissä. Sisäiselle hallintatunnukselle on mahdollista haluttaessa määrittää erikseen sekä kirjautumissalasana että enable-tilan salasana.

5.7 Hallinta

ACS-palvelinten hallintaa varten niillä on omat järjestelmänvalvojatunnukset. Yleisesti ottaen selainkäyttöliittymällä käytetäviä järjestelmänvalvojatunnuksia ei voi käyttää komentokehotepuolella (CLI Reference Guide for Cisco Secure Access Control System 5.3 2011, 2-3). ACS-palvelimen 5.3-versiossa järjestelmänvalvojatunnukset ovat aina sisäisiä eli niitä ei voida todentaa AD-palvelimelta (User Guide for Cisco Secure Access Control System 5.3 2011, 16-6). Cisco Systems suosittelee, että järjestelmänvalvojatunnukset sidotaan työntekijöiden henkilöllisyyteen (User Guide for Cisco Secure Access Control System 5.3 2011, 16-6). Järjestelmänvalvojatunnukset siirtyvät ensisijaisilta ACS-palvelimilta toissijaisille ACS-palvelimille. Kaikilla selainpohjaisilla järjestelmänvalvojatunnuksilla voi siten kirjautua kaikkien ACS-palvelinten selainliittymiin.

Järjestelmänvalvojatunnusten valtuudet riippuvat rooleista. Ensimmäisellä järjestelmänvalvojatunnuksella on aina SuperAdmin-rooli. Taulukossa 2 on esitelty ACS-palvelimen järjestelmänvalvojatunnusten mahdolliset eri roolit.

TAULUKKO 2. ACS-järjestelmävalvojaroolit (User Guide for Cisco Secure Access Control System 5.3 2011, 16-4-16-5)

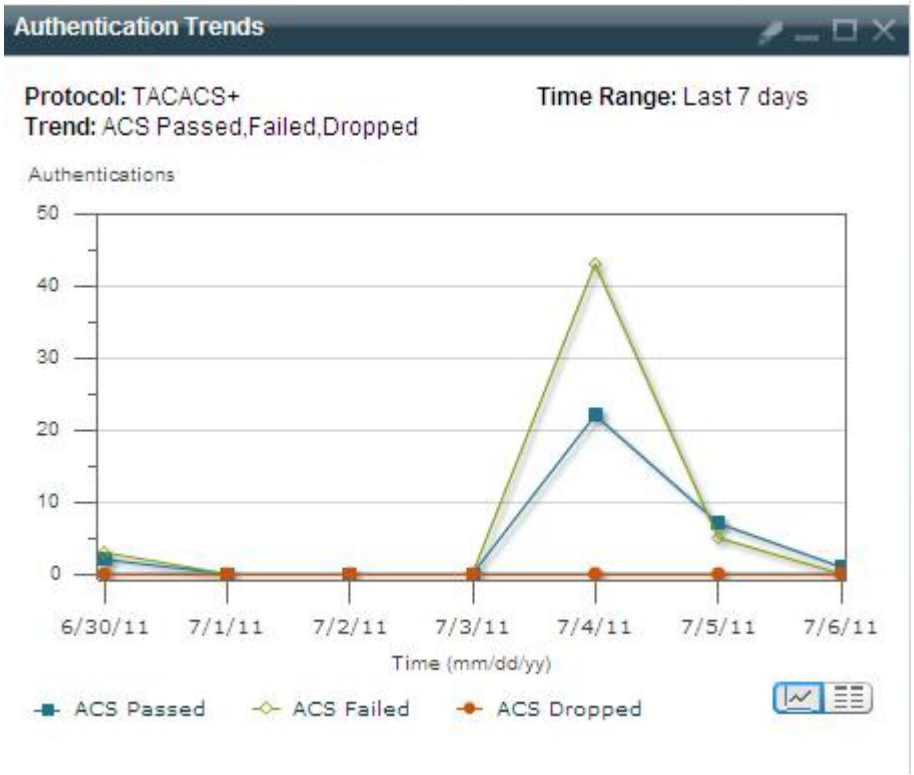
Rooli	Oikeudet
ChangeAdminPassword	Oikeus muuttaa muiden ACS-järjestelmänvalvojien salasanoja.
ChangeUserPassword	Oikeus muuttaa sisäisten hallintatunnusten salasanoja.
NetWorkDeviceAdmin	Oikeus muokata verkkolaiteluetteloa sekä NDG-ryhmiä.
PolicyAdmin	Oikeus muokata sääntöjen ehtoja sekä palveluita.
ReadOnlyAdmin	Lukuoikeus ACS-palvelimen kaikkiin asetuksiin.
ReportAdmin	Lukuoikeus Monitoring & Report Viewer -puolelle.
SecurityAdmin	Oikeus luoda, muokata ja poistaa järjestelmänvalvojien tunnuksia.
SuperAdmin	Täydet oikeudet ACS-palvelimelle.
SystemAdmin	Oikeudet hallita ACS-palvelimia.
UserAdmin	Oikeus hallita sisäisiä hallintatunnuksia.

Mikäli tietoverkon ylläpidossa on useita ACS-palvelimia hallinnoivia työntekijöitä, on suositeltavaa luoda SuperAdmin-järjestelmänvalvojatunnuksen lisäksi tunnus, jolla on ReportAdmin-rooli. Sitä käytetään kirjautuessa Monitoring & Report Viewer -palvelimelle.

Järjestelmänvalvojatunnuksien tietoihin on mahdollista laittaa sähköpostiosoite. ACS-palvelimen valvonta-asetuksiin on mahdollista määrittää hälytyskriteerien täyttyessä sähköpostiviestin lähettäminen valituille järjestelmänvalvojille.

5.8 Valvonta

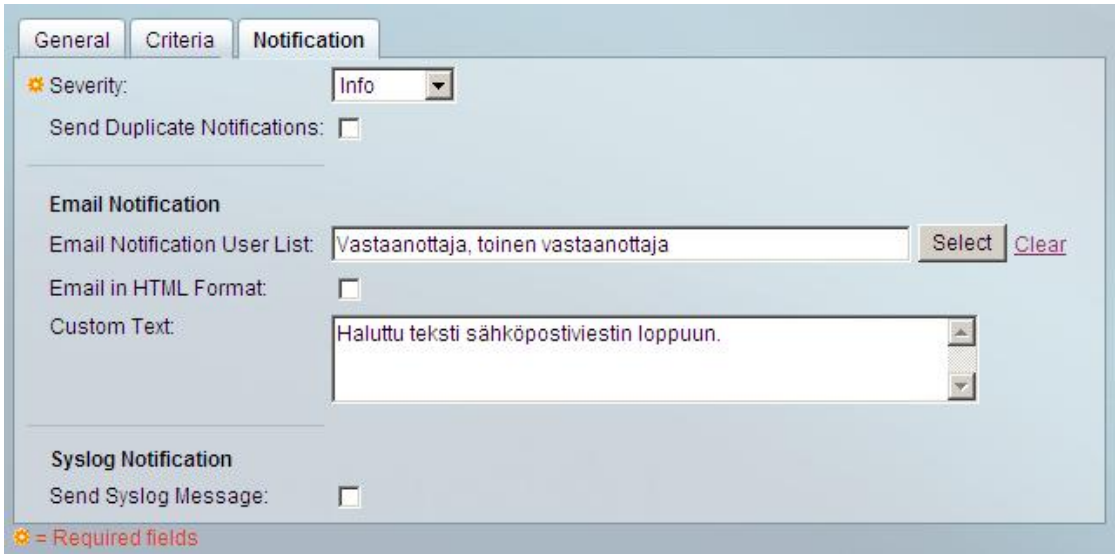
ACS-palvelin tarjoaa mahdollisuuden laitehallintatilanteen valvontaan Monitoring and Reports -näkymän avulla. Kuviossa 14 näkyy esimerkki näkymän tarjoamasta tiedosta. Näkymää voidaan käyttää myös tietoverkko-ongelmien havaitsemiseen.



KUVIO 14. Todennusnäkymä

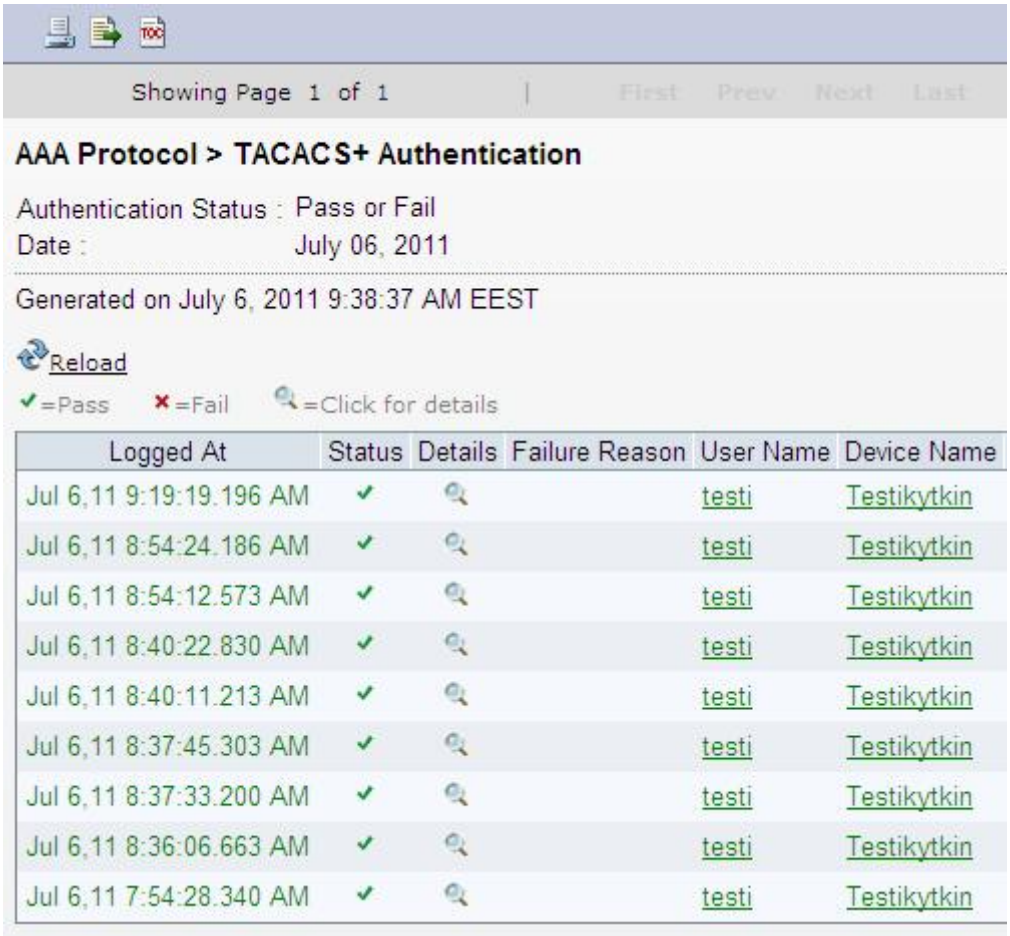
Monitoring and Reports -näkymään on mahdollista asettaa raja-arvoja hälytyksiä varten. Hälytykset tulevat näkyviin muun muassa etusivun dashboard-näkymään, missä niitä on mahdollista kommentoida ja kuitata suljetuiksi. Hälytyksiä voidaan

lähettää sähköpostilla järjestelmänvalvojille ja niihin voi asettaa oman viestin, kuten näkyy kuviosta 15.



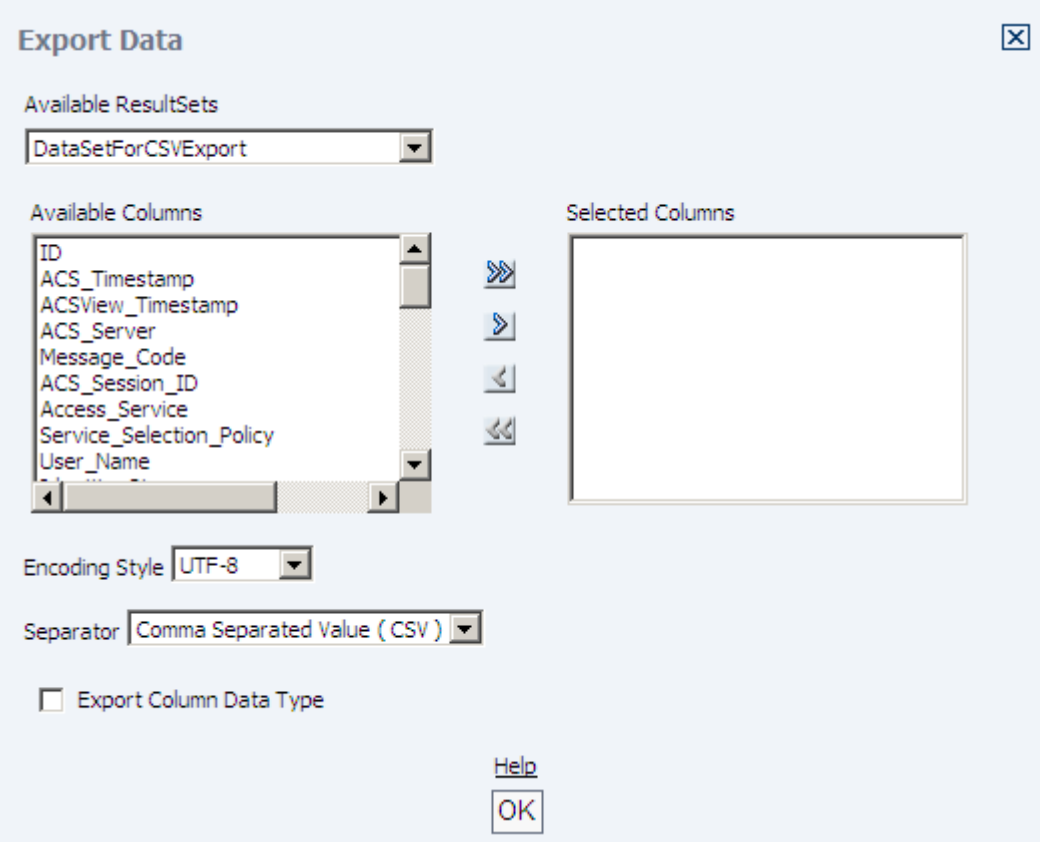
KUVIO 15. Sähköposti-ilmoitus

Valvottavia asioita voi olla esimerkiksi epäonnnistuneiden kirjautumisten määrä. Kuviossa 16 on näkymä tapahtuneista TACACS+-todennuksista. Yksittäisten todennusten tarkka tutkiminen onnistuu painamalla Details-sarakkeen suurennuslasia.



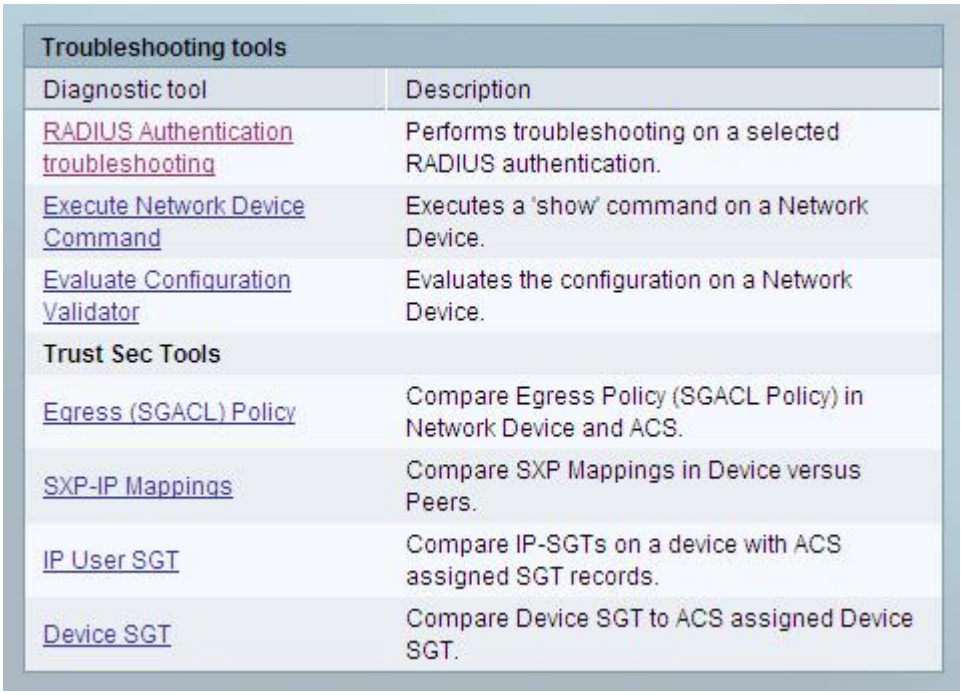
KUVIO 16. TACACS+-todennukset

Cisco Systemsin mukaan lokitietojen keräämiseen varattu ACS-palvelin on noin 50 % hitaampi käsittelemään todennuksia kuin tavallinen ACS-palvelin (Migration Guide for Cisco Secure Access Control System 5.3 2011, 1-7). Monitoring and Report Viewer -näkymän keräämät lokitiedot on mahdollista viedä csv-tiedostoksi kuvion 17 mukaisesti.



KUVIO 17. Tietojen vienti csv-tiedostoon

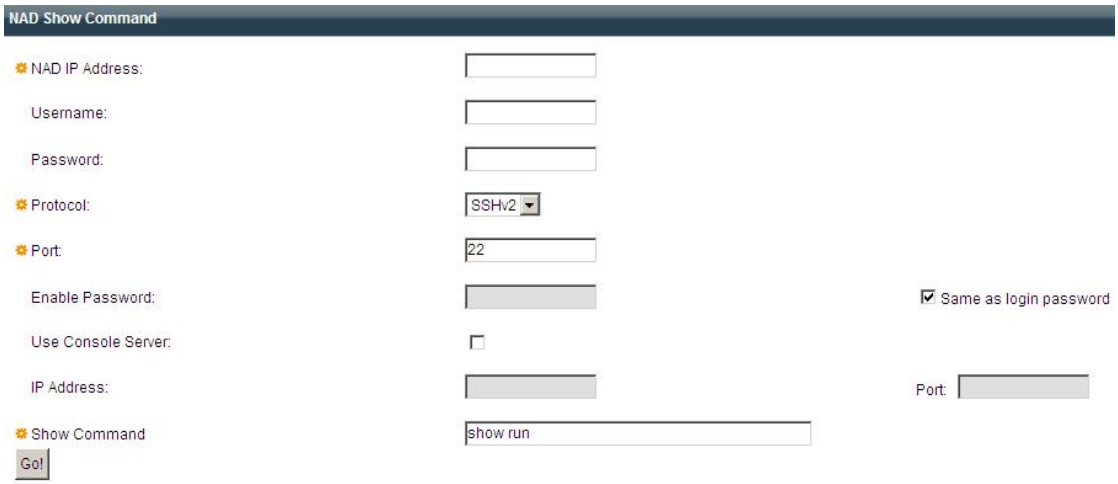
Monitoring and Report Viewer -näkymä sisältää ongelmanratkaisutyökaluja. Troubleshooting-otsikon alta löytyy yleisesti käytetyt tietoverkkotyökalut ping, traceroute ja nslookup. Kuviossa 18 näkyy Expert Troubleshooter -aliotsikon alta löytyviä lisätyökaluja syvälliseen tutkimiseen.



Troubleshooting tools	
Diagnostic tool	Description
RADIUS Authentication troubleshooting	Performs troubleshooting on a selected RADIUS authentication.
Execute Network Device Command	Executes a 'show' command on a Network Device.
Evaluate Configuration Validator	Evaluates the configuration on a Network Device.
Trust Sec Tools	
Egress (SGACL) Policy	Compare Egress Policy (SGACL Policy) in Network Device and ACS.
SXP-IP Mappings	Compare SXP Mappings in Device versus Peers.
IP User SGT	Compare IP-SGTs on a device with ACS assigned SGT records.
Device SGT	Compare Device SGT to ACS assigned Device SGT.

KUVIO 18. Expert Troubleshooter

Esimerkiksi NAD Show Command ja Execute Network Device Command -työkaluilla voidaan ajaa kytkimellä show run -komennon. Kuviossa 19 näkyy, kuinka toimenpide vaatii käyttäjältä joidenkin tietojen syöttämisen.



KUVIO 19. NAD Show Command

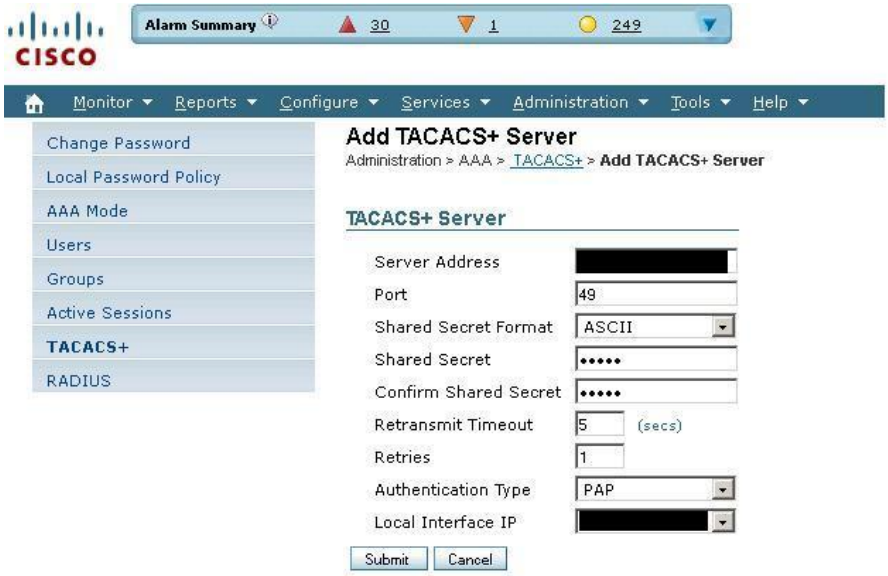
5.9 Varmuuskopiointi

ACS-palvelimen omat tietokannat sekä asetustiedostot voidaan varmuuskopioida aina tarvittaessa sekä halutun aikataulun mukaisesti. Varmuuskopio voidaan tallentaa paikallisesti ACS-palvelimelle tai tietoverkon kautta verkkokovalevylle joko FTP-, TFTP-, SFTP- tai NFS -protokollalla. Näistä SFTP on totetutettu SCP-protokollalla (Release Notes for Cisco Secure Access Control System 5.3. 2011, 5).

ACS-palvelimen omien tietojen lisäksi Monitoring and Reports -palvelimen keräämä lokitieto voidaan varmuuskopioida. Lokitietoja voidaan lisäksi varmuuskopioida pienin lisäyksin incremental backup -menetelmällä. Tällöin ACS- palvelin luo täyden lokikopion ja sen jälkeen pienempiä lisälokeja. Menetelmän etuja ovat nopeat varmuuskopioinnit sekä tallennuskapasiteetin tehokas käyttö, joten laitevalmistaja suosittelee sitä (User Guide for Cisco Secure Access Control System 5.3 2011, 15-3).

5.10 Yhteistoiminta Wireless Control System -sovelluksen kanssa

Wireless Control System on Cisco Systemsin sovellus langattomien tietoverkkojen hallintaan. ACS-palvelin voi toimia TACACS+-palvelimena WCS:lle, jolloin WCS-sovellukseen voidaan kirjautua sekä AD-käyttäjätunnuksilla että ACS-palvelimen sisäisillä käyttäjätunnuksilla. Kuviossa 20 näkyy WCS-sovelluksen TACACS+-sivu.



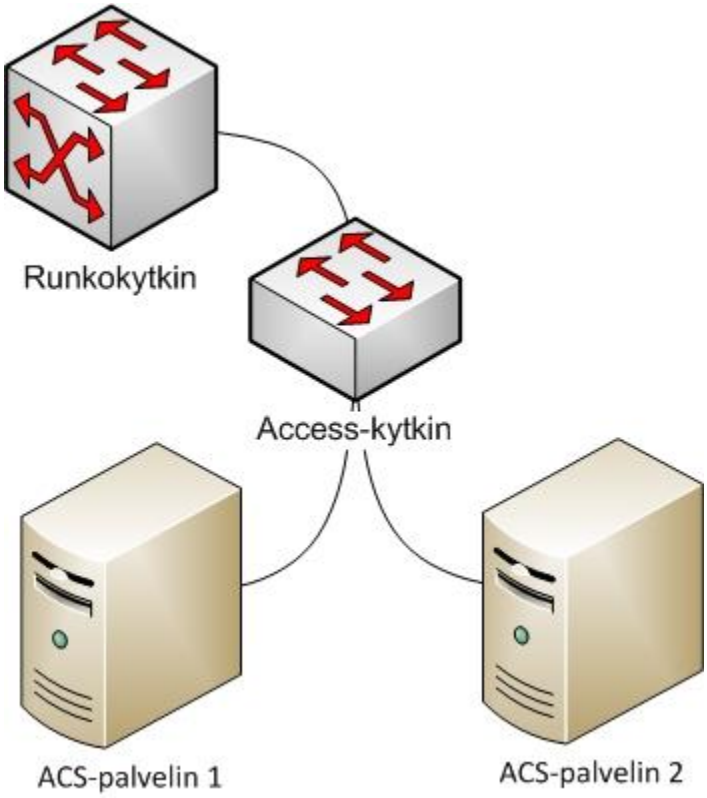
KUVIO 20. WCS ja TACACS+-palvelin

6 TOTEUTUS

ACS 5.2 -palvelimet saatiin kumpikin asennettua ja otettua käyttöön sairaanhoitopiirin tietoverkossa. 5.2-versiossa oli pieniä bugeja, joista osa korjaantui päivittämällä palvelimet 5.3-versioon. Yksi tälläinen bugi oli muun muassa traceroute-toiminto, joka ei toiminut 5.2-versiossa. Kaikki tehtävän kannalta oleelliset asiat toimivat kummassakin versiossa.

ACS-palvelimen ominaisuuksista muun muassa verkkotyökalut, varmuuskopiointi ja varmuuskopioiden palautus kokeiltiin toimiviksi. Erilaisia vikatilanteita mallinnettiin sulkemalla verkkoyhteyksiä, asettamalla tarkoituksella vääriä asetuksia sekä syöttämällä vääriä käyttäjätunnuksia.

ACS-palvelimet ovat koko ajan päällä pidettäviä laitteita. Opinnäytetyön tekemisen aikana niissä ei havaittu merkittäviä virhetilanteita. Ainoastaan yhden kerran 5.2-versioisessa ACS-palvelimessa kaikki prosessit eivät olleet päällä, mutta sekin korjaantui etäältä suoritetulla uudelleenkäynnistyksellä. Käyttöönotettujen ACS-palvelinten topologia on esitetty kuviossa 21.



KUVIO 21. ACS-palvelimet

ACS-palvelinten ja TACACS+-protokollan osalta päästiin tavoitteeseen. Yhteistyö kytkinten sekä ACS-, NTP- ja AD-palvelinten välillä toimi hyvin. Lisääntynyt tietoliikenne ei aiheuttanut huomattavaa aikaviivettä kytkinten hallinnassa. TACACS+-protokolla otettiin onnistuneesti tuotantokäyttöön myös Jyväskylän toimipisteen ulkopuolisilla kytkimillä.

Työasemien AD-pohjainen 802.1X-todennus saatiin toimimaan. Tarvittavat ACS-palvelimen säännöt sekä kytkinten asetukset saatiin selvitettyä. Kytkimet toimivat koekäytössä avoimessa tilassa ja kerryttivät lokia ACS-palvelimelle. MAB saatiin testattua toimivaksi menetelmäksi.

7 POHDINTA

Kokonaisuutena ACS-palvelimet toimivat hyvin. ACS-palvelimien käytön aikana törmättiin muutamaan vikaan, mutta ne eivät haitanneet olennaisesti kytkinten hallintaa TACACS+-protokollan avulla. Päivitys 5.3-versioon kannatti, mutta ei poistanut kaikkia havaittuja vikoja.

ACS-palvelinten graafinen käyttöliittymä valikoineen tuntui aluksi sekavalle, mutta sen oppi tuntemaan ulkoa tärkeimmiltä toiminnoiltaan muutamassa viikossa. Jatkossa verkkolaitteiden laitetietojen sekä MAC-osoitteiden lisääminen ACS-palvelimille on syytä tehdä csv-tiedostojen avulla vaiheen työläisyyden vuoksi. ACS-palvelinten määrä koettiin riittäväksi sekä vikatilanteiden varalta että tietoverkon kokoon nähden. Mallinnetuissa vikatilanteissa kytkinten hallinta hidastui. Aikaviive kasvoi merkittäväksi siinä tapauksessa, että kaikki ACS-palvelimet eivät olleet käytettävissä. Tällöinkään viive ei estänyt kytkinten hallintaa.

Työ eteni sysäyksittäin ja useasti etenemisnopeutta rajoitti tietojen puute tai jonkun tietyn ominaisuuden tarkan tuntemuksen puute. ACS-palvelimen oppaiden lisäksi oli toisinaan tarpeen tukeutua Cisco Systemsin omiin tukifoorumeihin.

TACACS+, 802.1X- ja RADIUS havaittiin toimiviksi protokolliksi, 802.1X:n ollessa näistä käyttöönotoltaan työläin. 802.1X synnytti myös ylivoimaisesti eniten verkkoliikennettä, mikä tulee ottaa huomioon jatkossa. Muutoksista tärkein oli onnistunut siirtyminen henkilöön sidottuihin käyttäjätunnuksiin sekä niiden myötä käyttäjäryhmään perustuvaan laitehallintaan. Samalla kytkinten komentojen lokimerkinnät ja työasemien todennusyritykset keskittyivät helposti luettevaan muotoon. Näin AAA-tilanne parantui olennaisesti Keski-Suomen sairaanhoitopiirin tietoverkossa.

LÄHTEET

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. & Levkowetz, H. 2004. RFC 3748 Extensible Authentication Protocol (EAP). Viitattu 26.10.2011. Http://www.ietf.org/rfc/rfc3748.txt.

Brown, E. 2007. 802.1X Port-Based Authentication. New York: Auerbach Publications.

Cisco Secure Access Control System 5.3. 2011. Laite-esittely Cisco Systemsin sivustolla. Viitattu 26.10.2011. Http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps5698/ps6767/ps9911/data_sheet_c78-683481.pdf.

CLI Reference Guide for Cisco Secure Access Control System 5.3. 2011. Cisco Systemsin ohje. Viitattu 26.10.2011. Http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/command/reference/cli.pdf.

Installation and Upgrade Guide for Cisco Secure Access Control System 5.3. 2011. Cisco Systemsin ohje. Viitattu 26.10.2011. Http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/installation/guide/csacs.pdf.

Introduction to IEEE 802.1X and Cisco® Identity-Based Networking Services (IBNS). 2008. Cisco Systemsin esite. Viitattu 26.10.2011. Http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/CiscoIBNS-Technical-Review.pdf.

Migration Guide for Cisco Secure Access Control System 5.3. 2011. Cisco Systemsin ohje. Viitattu 26.10.2011. Http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/migration/guide/Migration_Guide.pdf.

Release Notes for Cisco Secure Access Control System 5.3. 2011. Cisco Systemsin ohje. Viitattu 26.10.2011. Http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/release/notes/acs_53_rn.pdf.

Sankar, K., Sundaralingam, S., Balinsky, A. & Miller, D. 2005. Cisco Wireless LAN Security. Indianapolis: Cisco Press.

Santuka, V., Banga, P. & Carroll, B. 2011. AAA Identity Management Security. Indianapolis: Cisco Press.

Tägström, J. 2011. Ei vain puhetta & powerpoint esityksiä - 802.1x autentikoinnin käyttöönotto LAN-verkoissa NYT. Viitattu 26.10.2011. Http://www.tietoturvatapahtuma.fi/object/161b8d129a5df3b4109699e717dff1d2171.

User Guide for Cisco Secure Access Control System 5.3. 2011. Cisco Systemsin ohje. Viitattu 26.10.2011. Http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.3/user/guide/ACSuserguide.pdf.

LIITTEET

Liite 1. ACS-palvelimen käyttöönotto

Vaihe 1. alkutoimenpiteet konsoliyhteyden avulla

Asenna ACS-palvelin paikoilleen laitekaappiin. Tämän jälkeen laita ACS-palvelimeen virrat päälle ja kytke verkkoyhteys. Kytke DB9-kaapeli kannettavan tietokoneen sekä ACS-palvelimen takapaneelin oikeassa reunassa olevan sarjaportin välille. Sarjaportti on numeroitu kolmeksi Cisco Systemsin asennusohjeen kuviossa 2-4. (Installation and Upgrade Guide for Cisco Secure Access Control System 5.3 2011, 2-5). Anna konsoliyhteydellä komennot:

setup
isäntänimi
IP-osoite
aliverkon peite
oletusyhdyskäytävä
toimialue
NTP-palvelin 1
y
NTP-palvelin 2
järjestelmänvalvojatunnus
salasana
salasana uudestaan

Lopuksi ACS-palvelin käynnistyy uudelleen.

Cisco Systems suosittelee korkeintaan 15 merkin pituisia isäntänimiä (User Guide for Cisco Secure Access Control System 5.3 2011, 8-46). ACS-palvelimen käynnistyttyä uudestaan, kirjaudu sisään konsoliyhteydellä ja tarkista kaiken olevan oikein seuraavilla komennoilla:

sh application
sh application version acs
sh application status acs

Tässä välissä asetetaan oikeat aika-asetukset:

conf t

clock timezone EET

yes

ntp server IP-osoite-1 IP-osoite-2

exit

wr mem

reload

yes

y

show ntp

show clock

Voidaan myös luoda uusia käyttäjätunnuksia:

conf t

username nimi password plain salasana role admin

exit

wr mem

Vaihe 2. salasanan vaihto ja ACS-palvelimen lisenssointi

Ota https-yhteys ACS-palvelimeen ja kirjaudu sen GUI:n, minkä jälkeen vaihda oletus-salasana. Tämän jälkeen on asennettava ACS-palvelimen lisenssi valitsemalla Cisco Secure ACS License Registration. Ikkunaan avautuu harmaa kehys, joka kysyy Cisco-sivuston käyttäjätunnusta ja salasanaa. Tuotteen aktivointiavaimen syötön jälkeen tarkista, että Ciscon ehdottamat tiedot ovat oikein. Cisco lähettää lisenssin sisältävän LIC-tiedoston sähköpostiosoitteeseen ja saatu lisenssitiedosto asennetaan antamalla ACS-palvelimelle LIC-tiedoston polku. Jos asennat ensisijaista ACS-palvelinta, siirry vaiheeseen kuusi.

Vaihe 3. ACS-palvelimen asetus toissijaiseksi

Tämä vaihe tehdään, mikäli ensimmäinen ACS-palvelin on jo asennettu ja ollaan asentamassa toista ACS-palvelinta. Toissijaisella ACS-palvelimella: System Admin-istration > Operations > Local Operations > Deployment Operations. Syötetään ensisi-jaisen ACS-palvelimen IP-osoite sekä ACSAdmin-tunnus. Lopuksi painetaan Register

to Primary. Sen jälkeen ensisijaisella palvelimella: System Administration > Operations > Distributed System Management > Secondary Instances > tarkista, lukeeko toisen ACS-palvelimen kohdassa Replication Status Updated tai Pending. Kirjaudu toissijaiselle ACS-palvelimelle ja tarkista, ovatko asetukset kopioituneet sille. Jos kyllä, niin siirry vaiheeseen viisi. Jos ei, niin siirry seuraavaan vaiheeseen neljä.

Vaihe 4. asetusten kopiointi ensisijaiselta ACS-palvelimelta toissijaiselle ACS-palvelimelle
Tämä vaihe tehdään, mikäli ensimmäinen ACS-palvelin on jo asennettu ja ollaan asentamassa toista ACS-palvelinta. Mikäli vasta asennat ensimmäistä ACS-palvelinta, siirry vaiheeseen kuusi. Toissijaisella ACS-palvelimella: System Administration > Operations > Distributed System Management > valitse ACS-palvelin > Full Replication > OK > kirjaudu > System Administration > Operations > Distributed System Management > tarkista, että lukeeko näkymässä Updated tai Pending. Siirry vaiheeseen viisi.

Vaihe 5. ACS-palvelimen asetus Monitoring and reports -palvelimeksi
Tämä vaihe tehdään, mikäli ensisijainen ACS-palvelin on jo asennettu ja ollaan asentamassa ensimmäistä toissijaista ACS-palvelinta. Mene ensisijaisella ACS-palvelimella kohtaan: System Administration > Configuration > Log Configuration > Log Collector > Select Log Collector service >valitse toissijainen ACS-palvelin > Set Log Collector.

Tämän vaiheen jälkeen vain Monitoring and reports -palvelimella on mahdollista katsella lokitietoja. Mikäli ensisijaisella ACS-palvelimella yritettään avata Monitoring and reports -puolta, tulee selaimeen ilmoitus, että Internet Explorer ei voi näyttää WWW-sivua. Siirry seuraavaksi vaiheisiin 17 ja 18, joiden jälkeen toissijaisen ACS-palvelimen asetukset on tehty.

Vaihe 6. ensisijaisen ACS-palvelimen kytkeminen AD:hen
Tämä vaihe tehdään ACS-palvelimella, joka on valittu ensisijaiseksi ACS-palvelimeksi. Users and Identity Stores > External Identity Stores > Active Directory > syötetään tiedot, testataan yhteys painamalla Test Connection sekä painetaan lopuksi Save Changes. Onnistuneen AD-yhteyden jälkeen Active Directory -välilehdelle ilmestyy uudet välilehdet Directory Groups sekä Directory Attributes.

Vaihe 7. AD-ryhmien käyttöönotto

Tämä vaihe tehdään vain ensisijaisella ACS-palvelimella. Network Users and Identity Stores> External Identity Stores > Active Directory > Directory Groups > Select > haetaan halutut ryhmät Search Filterillä ja valitaan ne > OK > Save Changes. Valitut ryhmät ovat nyt käytettävissä sääntöjen ehtona.

Yksittäisten AD-tilien sekä konetilien ominaisuuksia voidaan myös poimia sääntäjen ehdoiksi. Network Users and Identity Stores > External Identity Stores > Active Directory > Directory Attributes > syötä käyttäjätunnus tai työasema muodossa host/isäntänimi > Select … > valitse haluttu ominaisuus > OK > Save Changes.

Vaihe 8. kytkinten ja muiden verkkoaitteiden lisääminen ACS-palvelimelle

Tämä vaihe tehdään vain ensisijaisella ACS-palvelimella. Laiteryhmät lisätään käsin: Network Resources > Network Device Groups > Location > Create > syötetään nimi, kuvaus sekä valitaan isäntäsijainti > Submit. Verkkolaitteiden laitetiedot lisätään csv-tiedostoa hyödyntäen: Network Resources > Network Devices and AAA Clients > File Operations > Add > Next > Download “Add “ Template > tallenna network_device_import_template.csv ja lisää siihen vaikkapa muistiolla tai Excelillä laitetiedot > Next > Selaa … > valitse tiedosto > Finish.

Vaihtoehtoisesti laitetiedot voidaan lisätä käsin: Network Resources > Network Device Groups > Device Type > Create > syötetään nimi, kuvas sekä valitaan isäntälaiteryhmä > Submit. Network Resources > Network Devices and AAA Clients > Create > syötetään nimi, kuvaus, IP-osoite (tai osoiteavaruus) > valitaan autentikoinniksi TACACS+ ja RADIUS sekä annetaan kummallekin Shared Secret >Submit.

Huomioi kummassakin menetelmässä, että Shared Secret voi olla korkeintaan 32 merkkiä pitkä (User Guide for Cisco Secure Access Control System 5.3 2011, 5-19).

Vaihe 9. Identity Groups

Tämä vaihe tehdään vain ensisijaisella ACS-palvelimella. Users and Identity Stores > Identity Groups > Create > syötetään vaaditut tiedot > Submit.

Vaihe 10. sisäiset hallintatunnukset

Tämä vaihe tehdään vain ensisijaisella ACS-palvelimella. Users and Identity Stores> Internal Identity Stores > Users > Create > syötetään vaaditut tiedot > Submit. Luodaan erikseen hallintatunnus omaa tilapäistä käyttöä varten sekä ulkopuolisia työntekijöitä varten. Mikäli ulkopuolisissa työntekijöiden joukossa on sellaisia, ketkä tarvitsevat toistuvasti kytkinten hallintatunnuksia, voidaan heille luoda nimetyt hallintatunnukset.

Vaihe 11. tunnistautumisjärjestysten asettaminen

Tämä vaihe tehdään vain ensisijaisella ACS-palvelimella. Users and Identity Stores > Identity Store Sequences > syötetään nimi ja kuvaus > valitaan Password Based > valitaan halutut tietokannat > Submit. Tunnistautumisjärjestyksiä voi tehdä useita eri tarpeita varten.

Vaihe 12. aikarajoituksen asettaminen

Tämä vaihe tehdään vain ensisijaisella ACS-palvelimella. Tämä vaihe on valinnainen siitä riippuen, että halutaanko ollenkaan rajata laitteiden hallintaa viikonpäivän tai kellonajan mukaan. Policy Elements > Session Conditions > Date and Time > Create > syötetään haluttu nimi ja kuvaus > valitaan alkamis- ja loppumisajankohdiksi Start Immediately sekä No End Date > valitaan kalenteristä viikkoaikataulu > Submit.

Vaihe 13. Authorization Profiles, Command Sets ja Shell Profiles

Tämä vaihe tehdään ensisijaisella ACS-palvelimella. Luodaan Authorization Profile erikseen jokaista 802.1X-käyttötarvetta kohden: Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Create > syötetään halutut tiedot > Submit. Mikäli halutaan asettaa kiinteä ohjaus tiettyyn VLAN-verkkoon, avataan halutun profiilin Common Tasks -välilehti > VLAN ID/Name > asetetaan seuraavat asetukset: Static ja Value-kohtaan VLAN-verkon numero > Submit.

Luodaan Command Set erikseen luku- sekä luku- ja kirjoitusoikeuksia varten: Policy Elements > Authorization and Permissions > Device Administration > Command Sets > Create > syötetään halutut tiedot > Submit.

Luodaan Shell Profile erikseen jokaista WCS-käyttötarvetta varten: Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create > syötetään halutut tiedot > avataan Custon Attributes -välilehti > lisätään halutun WCS-roolien ominaisuudet siten, että arvot Mandatory ja Static ovat valittuina > Submit. WCS-roolien tiedot löytyvät WCS-asetuksista: Administration > AAA > Groups > valitse haluttu rooli > Task List.

Vaihe 14. pääsypolitiikan luominen

Tämä vaihe tehdään ensisijaisella ACS-palvelimella. Access Policies > Access Services > Create > syötä nimi ja kuvaus > User Selected Service Type > Network Access tai Device Administration > Next > valitse tarvittavat protokollat > Finish. Access Policies > valitaan haluttu palvelu > Identity > Single result selection > Select > valitaan haluttu vaiheessa 11 luotu järjestys > Save Changes. Access Policies > Access Services > valitaan juuri luotu palvelu > Authorization > Create > syötetään tarvittavat ehdot ja puuttuvat ehdot saadaan edellisen tilan Customize-painikkeesta > kohtaan Results valitaan joko Authorization Profile, Command Set tai Shell Profile > OK. Luodaan erikseen yksi sääntö jokaista käyttötarvetta kohden: MAB, 802.1X, WCS, kytkinten laitehallinta ja niin edelleen.

Vaihe 15. palvelunvalintasäännöt

Tämä vaihe tehdään ensisijaisella ACS-palvelimella. Access Policies > Access Services > Service Selection Rules > Rule based result selection > Create > kohtaan Protocol valitaan joko match Tacacs tai match Radius > valitse muut halutut ehdot kuten esimerkiksi UseCase ja NDG:DeviceType > kohtaan Results valitse edellisessä vaiheessa 14 luotu palvelu > OK > Save Changes. Huomaa sääntöjen läpikäyntijärjestys sekä alhaalla näkyvä Default-sääntö, missä tulisi olla tuloksena DenyAccess.

Tässä vaiheessa voidaan kokeilla kirjautumista sellaiselle kytkimelle, jolle on asetettu liitteen 2 mukaiset asetukset. Pääsypolitiikasta riippuen kytkimen tulee hyväksyä sekä AD-käyttäjätunnukset että myös ACS-palvelimen sisäiset hallintatunnukset. Tarkista myös, että kirjautumistapahtumasta on syntynyt lokimerkintä Monitoring and Reports -näkymään.

Vaihe 16. paikallisten lokien säilytysajan kasvattaminen

Tämä vaihe tehdään ensisijaisella ACS-palvelimella. System Administration > Configuration > Log Configuration > Local Log Target > Local Log Target Settings > Maximum log retention period > syötä haluttu aika > Submit.

Vaihe 17. valvonnan sähköpostiviestien käyttöönotto

Ensin asetetaan ensisijaisella ACS-palvelimella järjestelmänvalvojatunnusten sähköpostiosoitteet: System Administration > Administrators > Accounts > valitaan haluttu järjestelmänvalvojatili > Edit > kohtaan Email Address syötetään yksi sähköpostiosoite > Submit.

Seuraavaksi asetetaan Monitoring and Reports -tehtävään valitulla toissijaisella ACS-palvelimella: Monitoring and Reports > Launch>Monitoring & Report Viewer > uudessa ikkunassa valitaan Monitoring Configuration > System Configuration > Email Settings > kohtaan Mail Server laitetaan oikean postipalvelimen isäntänimi ja kohtaan Mail From haluttu lähetysosoite > Submit.

Lopuksi on asetettava raja-arvo, jonka täyttyessä ilmoitus lähetetään. Tässä esimerkissä seurataan epäonnistuneita käyttäjätodennuksia: Monitoring and Reports > Alarms > Tresholds > valitaan ACS - System Errors > avataan Criteria-välilehti > valitaan kategoriaksi Failed Authentications. Raja-arvoiksi astetaan: Failed Authentications greater than 10 occurrences in the past 30 Minutes past for a User. Painetaan Submit ja mennään Notification-välilehdelle. Kohtaan Email Notification User List kirjoitetaan tai valitaan halutut järjestelmänvalvojat. Custom Text -kohtaan voidaan asettaa jokaisen viestin lopussa näkyvä teksti. Lopuksi painetaan Submit.

Vaihe 18. varmuuskopioinnin asettaminen

Viimeisessä vaiheessa otetaan varmuuskopiot kaikista ACS-palvelimista liitteen 6 ohjeiden mukaisesti. Lisäksi Monitoring and Report Viewer -palvelimella asetetaan Incremental Backup -varmuuskopiointi käyttöön: Monitoring and Reports > Launch Monitoring & Report Viewer > Monitoring Configuration > System Operations > Data Management > Removal and Backup > aseta varmuuskopiopalvelimet Data Reposito-

ry -kohdista > aseta tietojen säilytysaika sekä aikataulut > laita Incremental Backup On-asentoon > Submit.

Liite 2. Cisco Systemsin kytkinten TACACS+-asetukset

```
en
conf t
aaa new-model
tacacs-server host ip-osoite-1
tacacs-server host ip-osoite-2
tacacs-server key avain
aaa authentication login default group tacacs+ enable
aaa authentication enable default none
aaa accounting commands 0 default stop-only group tacacs+
aaa accounting commands 1 default stop-only group tacacs+
aaa accounting commands 15 default stop-only group tacacs+
aaa authorization config-commands
aaa authorization commands 0 default  group tacacs+ if-authenticated
aaa authorization commands 1 default  group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
exit
wr mem
```

Liite 3. Cisco Systemsin kytkinten ja Windows XP -työasemien 802.1X-asetukset

Kytkinten 802.1X-asetukset open mode ja MAB -tilassa

Huomaa in range -komento keskipaikkeilla.

```
en
conf t
ip device tracking
aaa authentication dot1x default group radius
aaa accounting dot1x default start-stop group radius
radius-server vsa send accounting
radius-server vsa send authentication
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
dot1x system-auth-control
aaa authorization network default group radius
radius-server host ip-osoite-1 key avain
radius-server host ip-osoite-2 key avain
in range portit
switchport mode access
authentication open
authentication port-control auto
mab
authentication event fail action next-method
authentication host-mode multi-auth
dot1x pae authenticator
authentication order dot1x mab
exit
wr mem
```

Kytkimen portteihin liitettyjen työasemien 802.1X-yhteensopivuuden voi kokeilla komennolla:

```
dot1x test eapol-capable in portti
```

802.1X-asetetuilla Windows XP -työasemilla tulee näkyviin kehoitus antaa käyttäjätunnukset alla olevan kuvion mukaisesti.

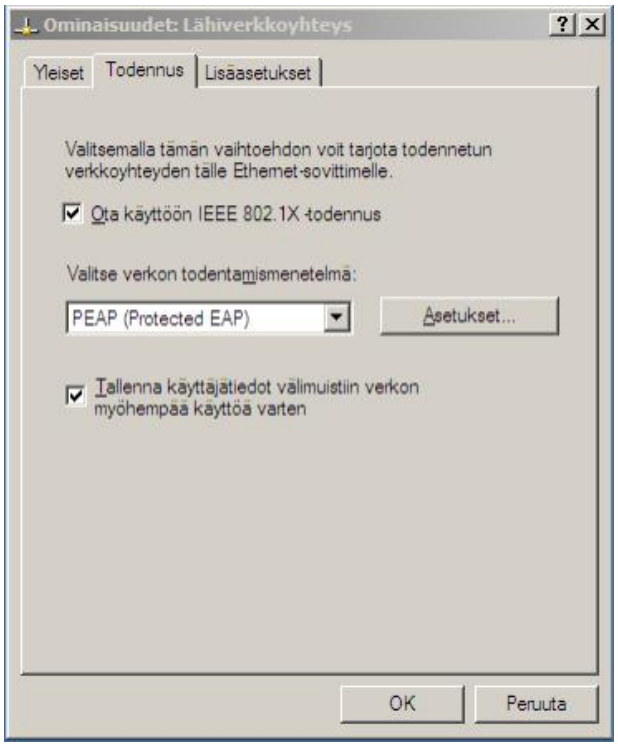
Windows XP -työasemien lankaverkon 802.1X-asetukset

Työasemalle kirjaudutaan järjestelmänvalvojatunnuksilla. Suorita-kehoitteeseen kirjoitetaan:

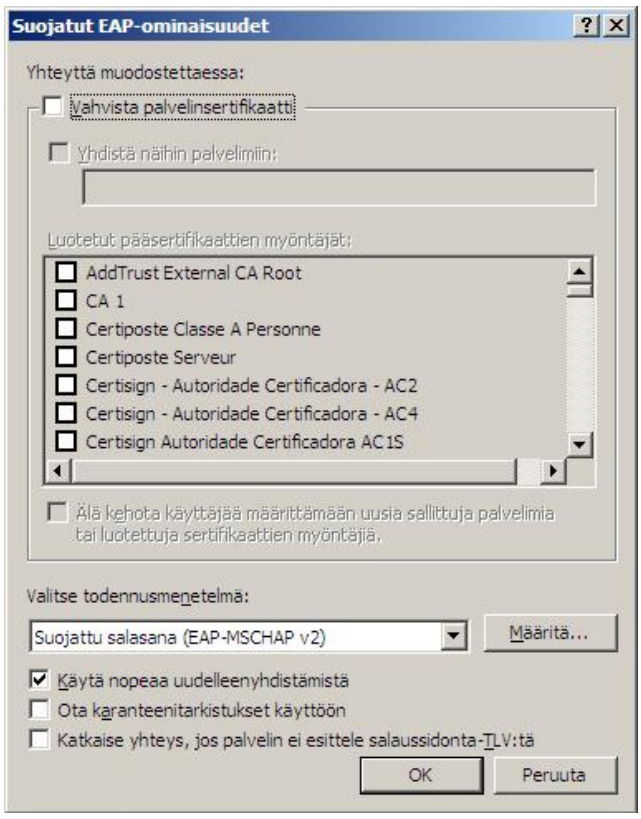
services.msc

Avautuneesta ikkunasta valitaan alhaalta Standardi-välilehti. Hiiren oikealla näppäimellä painetaan Automaattinen lankaverkon määrittäminen -palvelusta ja valitaan Käynnistä. Palvelut-ikkuna voidaan sulkea.

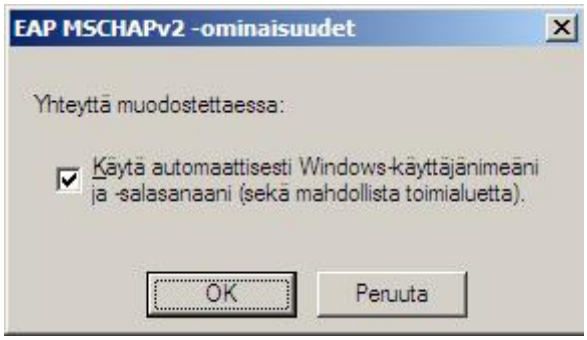
Siirrytään Ohjauspaneelin Verkkoyhteyksiin ja siellä painetaan hiiren oikealla näppäimellä haluttua verkkoyhteyttä. Valitaan Ominaisuudet ja avautuneesta ikkunasta toinen Todennus-välilehti. Laita Ota käyttöön IEEE 802.1X -todennus -ruutuun rasti seuraavan kuvion mukaisesti. Valitaan verkon todentamismenetelmäksi PEAP (Protected EAP) ja painetaan Asetukset….



Poistetaan rasti ruudusta kohdassa Vahvista palvelinsertifikaatti seuraavan kuvion mukaisesti. Valitaan todennusmenetelmäksi Suojattu salasana (EAP-MSCHAP v2).



Määritä…-kohdassa on rasti ruudussa alla olevan kuvion mukaisesti.



Windows XP -työasemien langattoman verkon 802.1X-asetukset

Siirrytään Ohjauspaneelin Verkkoyhteyksiin ja siellä painetaan hiiren oikealla näppäimellä haluttua verkkoyhteyttä. Valitaan Ominaisuudet ja avautuneesta ikkunasta toinen Langattomat verkot -välilehti. Valitse Ensisijaiset verkot -listasta haluamasi verkko ja Ominaisuudet. Avaa toinen Todennus-välilehti. Laita Ota käyttöön IEEE 802.1X -todennus -ruutuun rasti kuten lankaverkon 802.1X-asetuksissakin. Toimi samalla tavalla myös muiden 802.1X-asetusten kohdalla.

Liite 4. Ongelmatilanteita

Alla on lueteltu mahdollisia ongelmatiltanteita sekä niiden ratkaisut. Ratkaisut korostavat ongelman tilapäistä kiertämistä yksityiskohtaisen ratkaisun sijaan.

Kytkinten ja ACS-palvelimien välillä ei ole verkkoyhteyttä
Mikäli verkkoyhteys ACS-palvelimien ja kytkinten välillä ei toimi, kytkimet hyväksyvät paikallisen enable-salasanan. Käyttäjätunnus ohitetaan Enter-näppäimellä. Komentojen valtuutusasetusten vuoksi komentojen suorittamisessa on viidestä kymmeneen sekuntia kestävä viive, koska kytkimet yrittävät aina tavoittaa kummankin ACS-palvelimen.

Verkkoyhteyden toimiessa ACS-palvelimien, AD-palvelimien ja kytkinten välillä kytkimet hyväksyvät ACS- ja AD -käyttäjätunnukset, mutta eivät paikallista enable-salasanaa. Mikäli verkkoyhteydet ovat kokonaan poikki, kytkimet hyväksyvät konsoliyhteydellä paikallisen enable-salasanan.

AD-palvelimen ja ACS-palvelimien välillä ei ole verkkoyhteyttä
Verkkoyhteyden toimiessa vain ACS-palvelimien ja kytkinten välillä, kytkimet hyväksyvät ACS-palvelimelle luodut sisäiset käyttäjätunnukset. Niihin voidaan tukeutua myös siinä tilanteessa, jos AD-palvelimella on jotain muita vikoja kuin verkko-ongelmia.

ACS-palvelimet eivät toimi oikein
Verkkoyhteyden toimiessa ACS-palvelimien, AD-palvelimien ja kytkinten välillä, mutta ACS-palvelimien ollessa toiminnallisuudeltaan sekaisin, kytkimet eivät välttämättä hyväksy mitään käyttäjätunnuksia. Katkaise ACS-palvelimien ja kytkinten välinen verkkoyhteys, minkä jälkeen kytkimet hyväksyvät enable-salasanan. ACS-palvelin korjataan joko ottamalla konesalissa yhteys DB9-sarjaporttiin tai varaamalla sille sellainen verkkoalue, josta ei ole yhteyttä pääosalle hallinnoitavista kytkimistä.

Mikäli ensisijainen ACS-palvelin on pois käytöstä, voi olla tarpeen asentaa siihen uusi levykyva tai korvata se kokonaan uudella ACS-palvelimella. Tällöin uudelle ACS-

palvelimelle lisätään CLI-puolella varmuuskopiopalvelimen tiedot. Lopuksi sille palautetaan viimeisin toimiva varmuuskopio acs restore -komennolla (User Guide for Cisco Secure Access Control System 5.3 2011, 17-21).

Mikäli toissijainen ACS-palvelin on pitkän aikaa poissa käytöstä, käytetään ensisijaista ACS-palvelinta Monitoring and Reports -palvelimena. Mene ensisijaisella ACS-palvelimella kohtaan: System Administration > Configuration > Log Configuration > Log Collector > Select Log Collector service > valitse listasta ensisijainen ACS-palvelin > Set Log Collector. Mikäli jompikumpi ACS-palvelin joudutaan korvaamaan kokonaan uudella ACS-palvelimella, ota siinä tapauksessa huomioon kytkimille asetetut IP-osoitteet.

Kytkin ei anna suorittaa komentoja

Mikäli kytkin on asetettu ACS-palvelimen säännöissä väärään ryhmään, kytkin voi antaa kirjautua sisään normaalisti, mutta ei anna kuitenkaan suorittaa komentoja. Tarkista kytkimen tiedot ACS-palvelimelta.

Puuttuvat asetukset

Mikäli vain kytkimille on asetetty oikeat asetukset, kytkimet hyväksyvät vain paikallisen enable-salasanan. Tarkista, löytyvätkö kytkinten tiedot ACS-palvelimilta. Mikäli oikeat asetukset on asetettu vain ACS-palvelimille, kytkimet toimivat omien asetustensa mukaisesti.

Liite 5. Tyypillisiä Monitoring and Reports -virheilmoituksia

Selitykset perustuvat ACS-palvelimen koekäytön aikana tehtyihin havaintoihin.

12308 Client sent Result TLV indicating failure
Windowsin langattomassa verkkoyhteydessä on väärät asetukset. Oma tietokone > Ohjauspaneeli > Verkkoyhteydet > paina Langattoman verkkoyhteyden kuvaketta hiiren oikealla painikkeella > Ominaisuudet > Langattomat verkot -välilehti > valitse listasta kyseessä oleva langaton verkko > Ominaisuudet > Todennus-välilehti > Ominaisuudet > alhaalta pois rasti kohdasta: Katkaise yhteys, jos palvelin ei esittele salaussidonta-TLV:tä.

13030 TACACS+ authentication requet missing a User name
Käyttäjä painoi Enter-näppäintä kirjoittamatta käyttäjätunnusta.

13036 Selected Shell Profile is Deny Access
Tunnus ei vastannut mitään sellaista ehtoa, mikä sallisi sisäänpääsyn. Tarkista, meni-kö kirjautumisyritys ACS-palvelimen säännöissä Default-palveluun.

22040 Wrong password or invalid shared secret
Käyttäjä syötti väärän salasanan.

22056 Subject not found in the applicable indetity store(s)
Käyttäjätunnusta ei löydy määritellyistä sisäisistä tai ulkoisista tietokannoista. Vika voi olla myös siinä, että käyttäjätunnus on kyllä olemassa, mutta ACS-palvelimen säännöissä ei ole määritelty tarvittavia tietokantoja.

24207 Host disabled
ACS-palvelin tunnistaa verkkokortin MAC-osoitteen internal hosts -luettelosta, mutta osoite on Disabled-tilassa.

24401 Could not establish connection with ACS Active Directory Agent
Ilmoitus tulee jos käyttäjä on vaihtanut äskettäin käyttäjätunnuksensa salasanan. Käyttäjän tulisi kokeilla kirjautumista hetken kuluttua uudestaan.

24408 User authentication against Active Directory failed since user has entered the wrong password
Joko käyttäjä syötti väärään salasanan tai hänen AD-tunnuksensa ei ole todennussäännön vaatimassa ryhmässä.

24415 User authentication against Active Directory failed since user's account is locked out
AD-pohjainen käyttäjätunnus on lukossa, jolloin on voimassa arvo IdentityAccessRestricted = True.

24429 Could not establish connection with Active Directory
Ilmoitus tulee, jos käyttäjä on vaihtanut äskettäin käyttäjätunnuksensa salasanan. Käyttäjän tulisi kokeilla kirjautumista hetken kuluttua uudestaan. Ilmoitus tulee samassa tilanteessa kuin virheen 24401 ilmoitus.

Liite 6. ACS-palvelimen varmuuskopiointi ja päivittäminen

Varmuuskopiointi

Lisätään ensisijaiselle ACS-palvelimelle varmuuskopiopalvelimen tiedot: System Administration > Operations > Software Repositories > Create > syötä nimi, kuvaus ja muut tiedot > Submit. Seuraavaksi: System Administration > Operations > Local Operations > Deployment operations > Backup > syötä haluttu varmuuskopion nimen alkuosa > valitse kohdasta Repository varmuuskopiopalvelin > Submit. Otsikon Backup Options alla olevassa kohdassa voi olla valittuna ylempi vaihtoehto, mikä kopioi ACS-palvelimelle asetetut laite-, hallintatunnus- ja sääntötiedot. Alempi vaihtoehto kopioisi myös ACS-palvelimen omat laiteasetukset. Varmuuskopion ottaminen voidaan hoitaa myös CLI-puolella komennolla:
acs backup tiedosto repository nimi

Varmuuskopion palautus

Anna ensisijaisen ACS-palvelimen CLI-puolella komennot:
acs restore tiedosto.tar.gpg repository nimi
yes
ACS-palvelin käynnistää toimintonsa uudestaan. Tämän jälkeen on tarpeen tehdä vielä toissijaisen ACS-palvelimen irroitus ACS-palvelinryhmästä ja uudestaan liittäminen siihen (User Guide for Cisco Secure Access Control System 5.3 2011, 17-8).
Mene ensisijaisen ACS-palvelimen GUI-puolella kohtaan: System Administration > Operations > Distributed System Management > valitse toissijainen ACS-palvelin > Deregister. Mene toissijaisella ACS-palvelimella kohtaan: System Administration > Operations > Local Operations > Deployment Operations > Deregister from Primary. Mene uudestaan samalle sivulle, mutta tällä kertaa syötä ensisijaisen ACS-palvelimen IP-osoite sekä admin-tunnuksen tiedot. Valitse Hardware Replacement ja syötä toissijaisen ACS-palvelimen isäntänimi. Lopuksi paina Register to Primary.

Päivittäminen

ACS-palvelinten patch-päivityspaketit asennetaan ja poistetaan CLI-komentoliittymää käyttäen ja vaativat ACS-palvelimen uudelleenkäynnistämisen. ACS-palvelimelta kestää puolestatoista minuutista kahteen minuuttiin käynnistyä uudelleen. Päivityspake-

tin asennus on tehtävä erikseen jokaiselle ACS-palvelimelle. Päivitykset sisältävät aina aiempien päivitysten muutokset.

Päivityspaketin asennus:

acs patch install tiedosto repository nimi

yes

Päivityspaketin poistaminen:

acs patch remove tiedosto

ACS-palvelimen versio tarkistetaan komennolla:

sh version