NIST SPECIAL PUBLICATION 1800-9C

Access Rights Management for the Financial Services Sector

Volume C:
How-to Guides

James Banoczi
National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards
Nedu Irrechukwu
Josh Klosterman
Harry Perper
Susan Prince
Susan Symington
Devin Wynne
The MITRE Corporation
McLean, VA

August 2017

DRAFT

This publication is available free of charge from:
https://nccoe.nist.gov/projects/use-cases/access-rights-management

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-9C Natl. Inst. Stand. Technol. Spec. Publ. 1800-C, 276 pages, August 2017 CODEN: NSPUE2

FEEDBACK

You can improve this guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

Comments on this publication may be submitted to: financial_nccoe@nist.gov

Public comment period: August 31, 2017 through October 31, 2017

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov.

NIST CYBERSECURITY PRACTICE GUIDES

NIST Cybersecurity Practice Guides (Special Publication Series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

The documents in this series describe example implementations of cybersecurity practices that businesses and other organizations may voluntarily adopt. These documents do not describe regulations or mandatory practices, nor do they carry statutory authority.

ABSTRACT

Managing access to resources (data) is complicated because internal systems multiply and acquisitions add to the complexity of an organization's IT infrastructure. Identity and access management (IdAM) is the set of technology, policies, and processes that are used to manage access to resources. Access rights management (ARM) is the subset of those technologies, policies, and processes that manage the rights of individuals and systems to access resources (data). In other words, an ARM system enables a company to give the right person the right access to the right resources at the right time. The goal of this project is to demonstrate an ARM solution that is a standards-based technical approach to coordinating and automating updates to and improving the security of the repositories (directories) that maintain the user access information across an organization. The coordination improves cybersecurity by ensuring

that user access information is updated accurately (according to access policies), including disabling accounts or revoking access privileges as user resource access needs change. Cybersecurity is also improved through better monitoring for unauthorized changes (e.g., privilege escalation). The system executes user access changes across the enterprise according to corporate access policies quickly, simultaneously, and consistently. The ARM reference design and example implementation are described in this NIST Cybersecurity "Access Rights Management" practice guide. This project resulted from discussions among NCCoE staff and members of the financial services sector.

This *NIST Cybersecurity Practice Guide* also describes our collaborative efforts with technology providers and financial services stakeholders to address the security challenges of ARM. It provides a modular, open, end-to-end example implementation that can be tailored to financial services companies of varying sizes and sophistication. The use case scenario that provides the underlying impetus for the functionality presented in the guide is based on normal day-to-day business operations. Though the reference solution was demonstrated with a certain suite of products, the guide does not endorse these specific products. Instead, it presents the NIST Cybersecurity Framework (CSF) core functions and subcategories, as well as financial industry guidelines, that a company's security personnel can use to identify similar standards-based products that can be integrated quickly and cost-effectively with a company's existing tools and infrastructure. Planning for deployment of the design gives an organization the opportunity to review and audit the access control information in their directories and get a more global, correlated, disambiguated view of the user access roles and attributes that are currently in effect.

KEYWORDS

Access; authentication; authorization; cybersecurity; directory; provisioning.

ACKNOWLEDGMENTS

We are grateful to the following individuals for their generous contributions of expertise and time.

Name	Institution
Jagdeep Srinivas	AlertEnterprise
Hemma Prafullchandra	HyTrust
Roger Wigenstam	NextLabs
Don Graham	Radiant Logic
Adam Cohen	Splunk
Clyde Poole	TDi Technologies
Dustin Hayes	Vanguard Integrity Professionals

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Product Vendor	Component Name	Function
AlertEnterprise	Enterprise Guardian	Access policy management, administration and account provisioning system
HyTrust	Cloud Control	Privileged user access controller, monitor, and logging system for VSphere
NextLabs	NextLabs	Attribute based access control interface for SharePoint
Radiant Logic	RadiantOne	Virtual directory system
Splunk	Enterprise	Log aggregation and analytics system
TDi Technologies	ConsoleWorks	Application and operating system privileged user access controller, monitor, and logging system
Vanguard Integrity Professionals	Vanguard	Mainframe RACF to LDAP interface system

Contents

List of Tables

List of Figures

1 Introduction

The NIST Cybersecurity Practice Guide shows IT professionals and security engineers how we implemented this example solution. In Volume C we cover all the products employed in the reference design. We do not re-create the product manufacturers' documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our environment.

Note: These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this example implementation.

1.1 Practice Guide Structure

This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides users with the information they need to replicate this access rights management (ARM) approach. The reference design is modular and can be deployed in whole or in parts.

The guide contains three volumes:

- NIST SP 1800-9a: *Executive Summary* — High-level overview
- NIST SP 1800-9b: Approach, Architecture, and Security Characteristics—What we built and why
- NIST SP 1800-9c: *How-To Guides*—Instructions for building the example implementation **(you are here)**

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief security and technology officers will be interested in the *Executive Summary (NIST SP 1800-9a)*, which describes the:

- challenges identified by financial services companies
- operational benefits of adopting the solution
- high-level solution description

Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in the *Approach, Architecture, and Security Characteristics (NIST SP 1800-9b)* part of the guide, which describes what we did and why. The following sections will be of interest:

- Section 3.4.1, Assessing Risk Posture, describes the risk analysis we performed.
- Section 3.4.2, Security Control Map, maps the security functions and control of this example implementation to cybersecurity standards and best practices.

IT professionals who want to implement an approach like this will find the whole Practice Guide useful. The guide's information will provide insight into the resources and skills needed to implement an ARM solution. You can use the How-To portion of the guide, NIST SP 1800-9c (which is this document), to replicate all or parts of the example implementation created in our lab. *NIST SP 1800-9c* provides

specific product installation, configuration, and integration instructions for implementing the example implementation. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products in our environment to create an example implementation.

The guide assumes that IT professionals have experience implementing security products within the enterprise. Though we have used a suite of commercial products to address the challenge, this guide does not endorse these particular products. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of the solution. Your organization's security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices.

A *NIST Cybersecurity Practice Guide* does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to financial_nccoe@nist.gov.

1.2 Build Overview

The build is an example implementation of an access rights management system. The main components of the system include policy management, policy administration, access information provisioning, and security monitoring. In addition to these components, we have included privileged access management to secure the administration of the main components.

Security of the implementation is provided through logging changes to account/access information within the directories, a virtual directory, the policy administration system, and the privileged access management systems. The virtual directory is used to cache (mirror) the contents of the directories by checking for changes every 60 sec. All changes are reported to the security monitoring system immediately. Analytics within the security monitoring system (log collection and monitoring) correlates incoming logs. Security analysts are alerted when the analytics identify potential security events caused by inconsistent logs. Furthermore, the security analysts can drill down and investigate the cause of any alert. The available information within the security monitoring system enables them fully analyze the logs causing the alert and determine a course of action to effectively mitigate the cybersecurity incident. In addition, the directory monitoring provides another tool to monitor for malicious insider activity.

1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

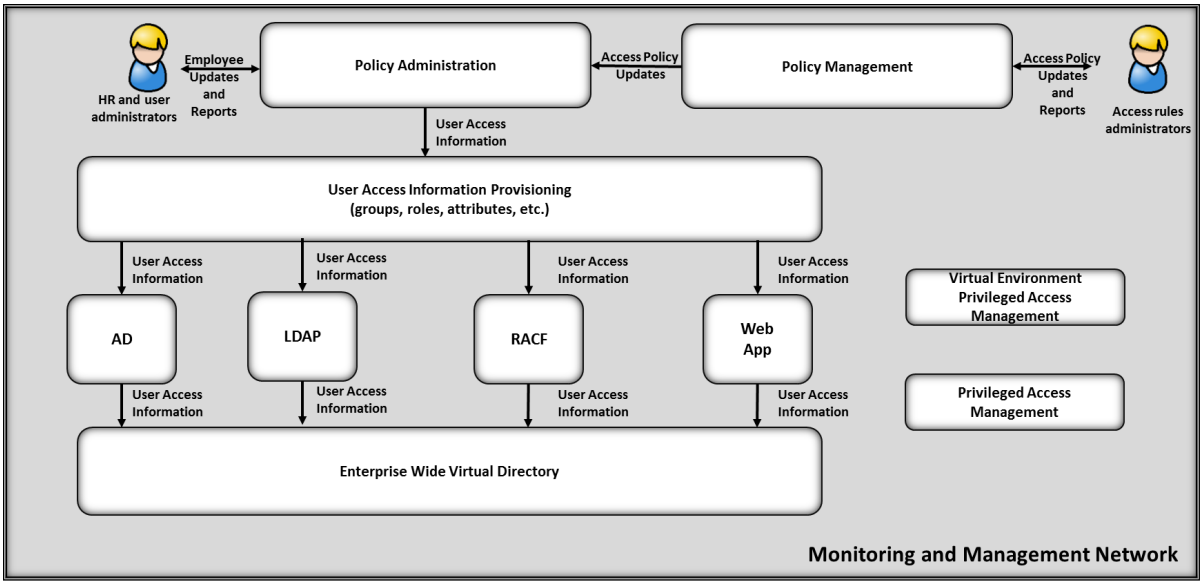
Typeface/ Symbol	Meaning	Example
Italics	filenames and pathnames	For detailed definitions of terms, see the *NCCoE Glossary.*

Typeface/ Symbol	Meaning	Example
	references to documents that are not hyperlinks, new terms, and placeholders	
Bold	names of menus, options, command buttons and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov

1.4 Logical Architecture Summary

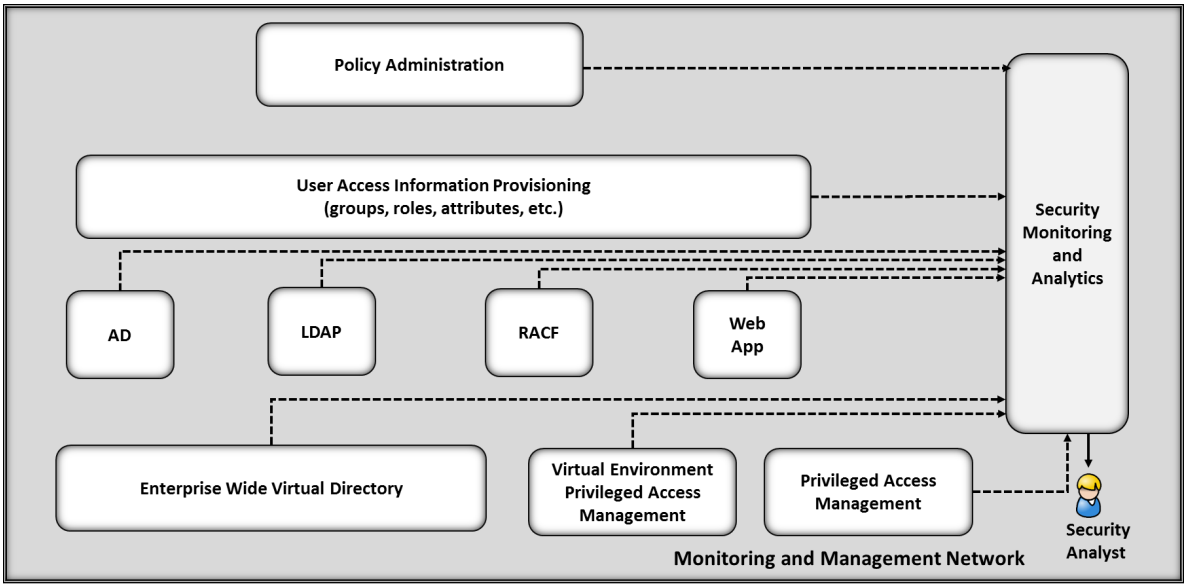
NIST Special Publication 1800-9b (SP1800-9b) describes an example implementation consisting of user access management (including provisioning) and security monitoring / data collection. SP1800-9b includes a much more detailed description of the architecture for building an instance of the example implementation using commercial products. That architecture is depicted in Figure 1-1 and Figure 1-2.

266 **Figure 1-1 Logical Access Rights Management Lab Build Architecture**



267

268 **Figure 1-2 Logical Security Log Collection and Monitoring Lab Build Architecture**



269

270 This volume of the practice guide provides detailed instructions on installing, configuring, and
271 integrating the products used to build an instance of the example solution. The role of each product in
272 the example implementation is described in SP1800-9b, Section 4, Architecture.

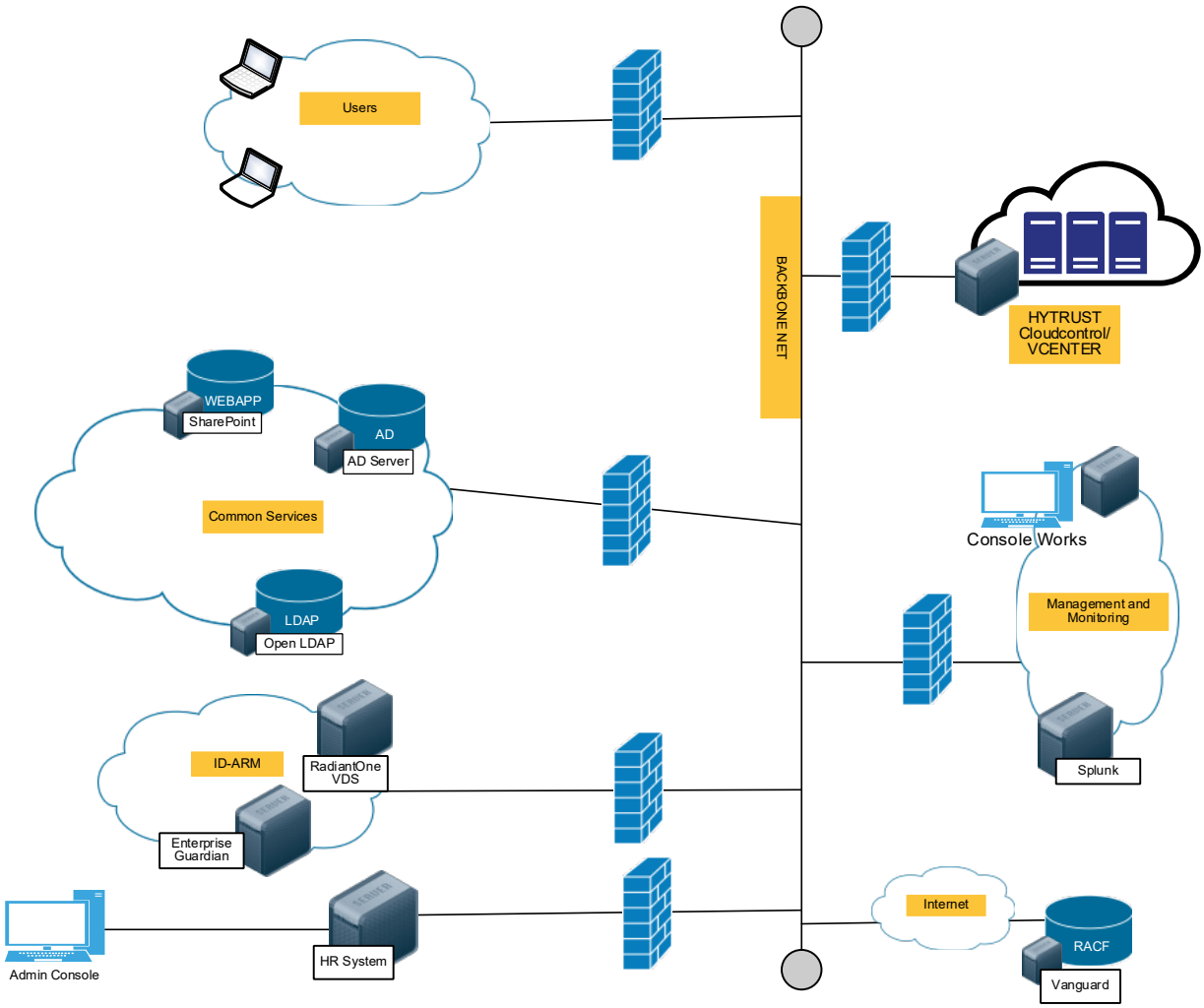
273 1.5 Network Diagrams

274 The architecture diagrams in the previous section present the logical connections needed among the
275 products used to build an instance of the example implementation. This section describes the virtual
276 environment lab implementation depicting the connectivity among the products.

277 1.6 NCCoE Lab

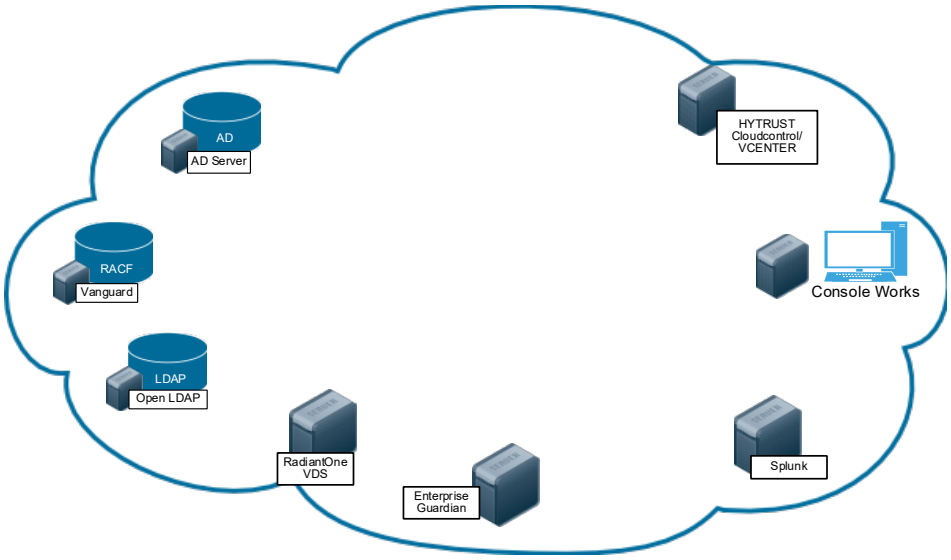
278 Figures 1-3 and Figure 1-4 show the network configurations used in the example implementation.

279 **Figure 1-3 NCCoE Lab Networking Diagram**



280

281 **Figure 1-4 NCCoE Lab Networking Diagram**



282

283 The following table includes the IP addresses for each of the networks depicted in Figure 1-3 and Figure
284 1-4.

285 **Table 1-1 NCCoE Lab Network and System IP Addresses**

Network	System	IP Address
Logging Network: 192.168.17.0/24	Splunk	192.168.17.10
Vendor Network: 10.33.50.0/16	ConsoleWorks	10.33.50.164
Common Services Network : 192.168.19.0/24	ActiveDirectory	192.168.19.10
	OpenLDAP	192.168.19.11
ID-ARM: 192.168.14.0/24	AlertEnterprise	192.168.14.113
	RadiantOne VDS	192.168.14.111
Vanguard: 172.17.212.0/24	VanguardMainframe	172.17.212.10
HyTrust: 192.168.20.0/24	CloudControl	192.168.20.11
	ESXiServer	192.168.20.12
Users: 192.168.15.0/24	User 1	192.168.15.110
	User 2	192.168.15.111
	HR1	192.168.15.112

2 Product Installation Guides

This section of the practice guide contains detailed instructions for installing and configuring all the products used to build an instance of the example implementation Product installation information is organized alphabetically by vendor, with one section for each instance of the product.

2.1 AlertEnterprise

AlertEnterprise Enterprise Guardian is an identity and access management system that provides end to end automated account provisioning, account change management, policy enforcement, and account administration across multiple diverse account directory systems.

2.1.1 How It's Used

AlertEnterprise Enterprise Guardian is used in the example implementation to provide access policy management, account change logging/reporting, account administration and account provisioning. Provisioining accounts includes creating new accounts and changes to existing accounts, including disabling accounts within multiple directories simultaneously.

2.1.2 Virtual Machine Configuration

The AlertEnterprise virtual machine consists of a Windows Server 2012 R2 configured as follows:

- Windows Server 2012 R2
- 1 CPU
- 2 NICs
- 32GB Mem
- 190GB Storage

Network Configuration (Interface 1)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.14.113
Netmask: 255.255.255.0
Gateway: 192.168.14.1
DNS Name Servers: 192.168.19.10
DNS-Search Domains: acmefinancial.com

Network Configuration (Interface 2)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.17.114
Netmask: 255.255.255.0
Gateway: 192.168.17.1
DNS Name Servers 192.168.19.10
DNS-Search Domains: acmefinancial.com

2.1.3 Prerequisites

Before starting the installation of the Enterprise Guardian Application, you must install the prerequisite software, which consist of a compatible version of JRE, Apache Activemq, and a SQL database. You will also need a supported internet browser and zip extracting software. See the *AlertEnterprise System Requirement Specifications Guide* (provided by vendor) for a full list of supported prerequisite software.

Prerequisite software used in this build:

- JRE 1.6 Update 22
- Apache Tomcat 6.0.26
- Oracle SQL Database 12c
- Google Chrome 55.0.2883.87
- 7-zip 16.04

2.1.4 Java

1. Download and install Java from the Oracle web site.
2. Make sure that JAVA_HOME variable is set to the folder where Java is installed and `%JAVA_HOME%/bin` is in the system's path.
3. Open the Command Prompt in Administrator Mode (right-click > Run as Administrator) and issue:

   ```
   Set JAVA_HOME=<PATH OF JDK/JRE>
   ```

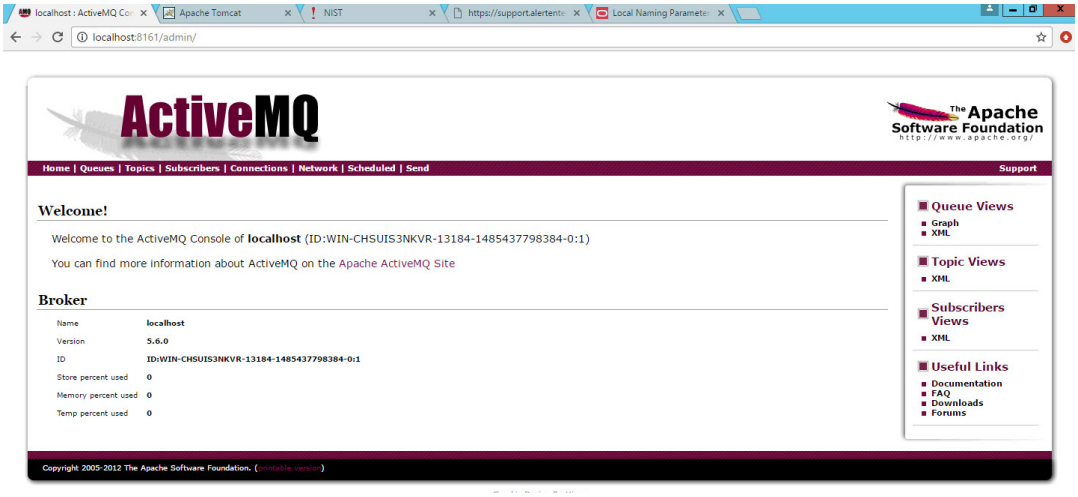
   Where <> is the path where Java is installed, for example, `C:\Program Files\Java\JRE6`
4. Setting Path:
   `PATH= C:\Program Files\Java\JDK1.6.0-21\bin;%PATH%`
5. Checking JAVA_HOME and PATH:

   ```
   Echo %JAVA_HOME%
   Echo %PATH%
   ```

2.1.5 Apache Activemq

1. Install the Activemq server according to documentation found on the Apache website.
2. Run ActiveMQ as a Windows service.
3. Ensure the server is installed correctly and running by connecting to the admin console on port 8161. For example: `URL: <IP address of the server where Active MQ is 2130`

installed>:8161/admin



2.1.6 Oracle DB

1. Install the Oracle SQL database according to documentation found on the Oracle website.
2. Ensure the pdborcl pluggable database service name is added correctly in the tnsnames.ora file per the Oracle documentation.

3. Open a command prompt and test by connecting with this command: **`sqlplus sys/<password>@pborcl as sysdba.`**

2.1.7 7-Zip

1. Download and install 7-Zip from www.7-zip.org.

2.1.8 Installation

You can install the AlertEnterprise Enterprise Guardian Application in three steps. This information is also found within the *AlertEnterprise Installation Guide*.

1. Install and Configure the Apache Tomcat Server.

2. Configure the database server.
3. Deploy the application.

2.1.9 Install and Configure Tomcat

1. Install the Apache Tomcat Server per the documentation found on the Apache website. Details can also be found within the *AlertEnterprise Enterprise Guardian Install Guide*.
    a. During the installation, specify the destination folder as **C:\AlertEnterprise\Tomcat.**
2. When installation is complete, navigate to **Start>Programs>Configure Tomcat** and select the **Java** tab.
3. Add the following lines to the end of Java Options, ensuring there are no spaces:

```
-XX:PermSize=1024
-Xms2048m
-Xmx2048m
-Dcom.alnt.fabric.loadInitData=force
"                                                    "--Dalert.db.update=update
```

4. Click **Apply** and **OK** to close the dialog box.

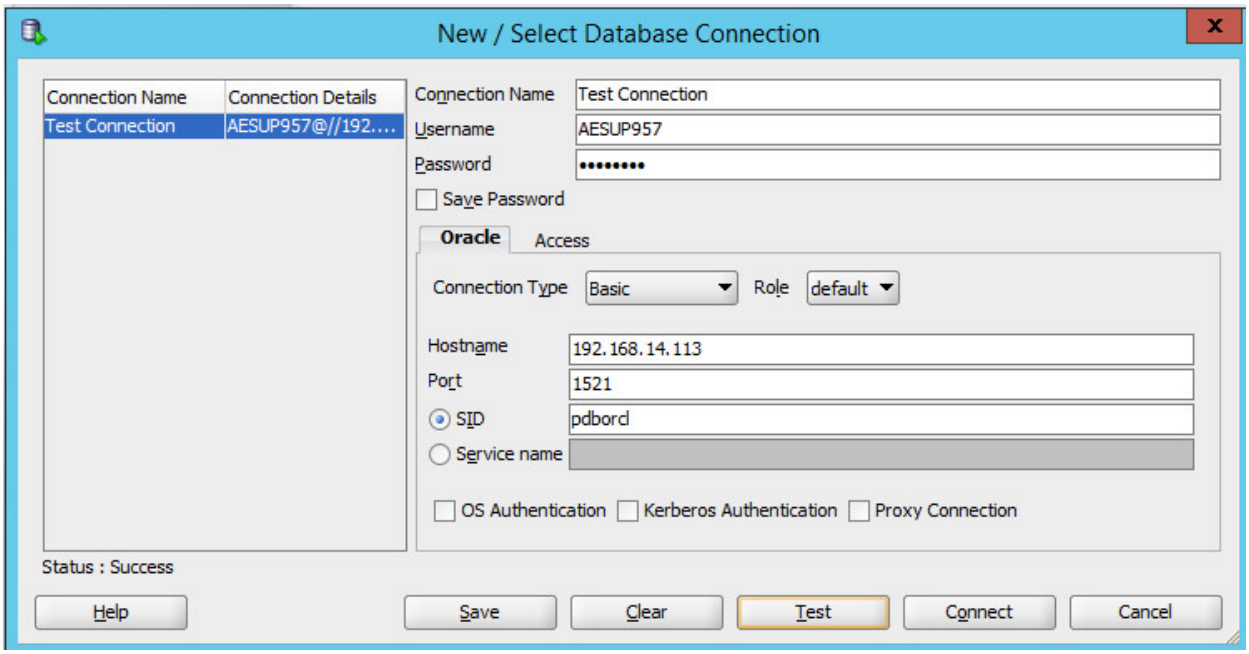
2.1.10 Configure the Database Server

The NCCoE build supports Oracle SQL Database 12c. See the administrator's guide for the full installation and configuration guide. Open a command prompt with administrator privileges and connect: **`sqlplus sys/<password>@pborcl as sysdba`**

1. Create a new schema/SID per your naming convention: **`create user <user/schema name> identified by <password>`**, you may have to unlock the schema: **`alter user <user/schema name> identified by <password> unlock`**
2. Use **`grant <attribute> to <user/schema name>;`** to grant the new user all of the following attributes:

    connect; resource; create synonym; create session; create sequence; create view; unlimited tablespace; create procedure; create trigger; create table

3. You can use Oracle SQL Developer to test the connection using the username and password created in Step 2. When this connection is successful, you can proceed.



2.1.11 Deploying the Application

After you have successfully configured the database, proceed to deploy the AlertEnterprise product on your web application server. The following deployment steps are required for the Tomcat 6.0 version:

Note: For steps required to use the SAP system connector or MySQL database, see the vendor documentation.

1. Stop the Tomcat server from the Windows services if it is already running. Click **Start > Run** and type `services.msc` then click **OK**. Select the Apache Tomcat and click the **Stop Service** icon to stop the service.
2. Copy the `AlertEnterprise.war, AccessMap.war` (if you possess AlertInsight license), `AlertEnterpriseHelp.war`, and `jasperserver-pro.war` files to the `<Tomcat installation folder>\webapps\` path.
3. If you have a license for the Password Management application, you need to copy the password management war file (`AIPM.war`) to `<Tomcat installation folder>/webapps.`
4. Create new folders `AlertCommonLib` and `AlertExternalLib` under the `<Tomcat Installation Folder>.`
5. Extract `AlertCommonLib.zip` under the `AlertCommonLib` folder. You will see many new files in this folder.
6. Edit `<Tomcat Installation Folder>\conf\catalina.properties` using any editor and add `common.loader` as described below:
   `common.loader=${catalina.base}/lib,${catalina.base}/lib/*.jar,${catalina.home}/lib,${catalina.home}/lib/*.jar,${catalina.home}/AlertCommonLib/*.jar,${catalina.home}/AlertExternalLib/*.jar .` Save the file and close the editor.

7. Add Database Connection. Add a new resource entry as below with name `jdbc/alntdb` in `<Tomcat installation folder>\conf\context.xml`. Replace the code in <> with relevant information.

   For ORACLE:

```
<Resource description="DB Connection"
name="jdbc/alntdb" auth="Container"
type="com.mchange.v2.c3p0.ComboPooledDataSource"
factory="org.apache.naming.factory.BeanFactory"
user=<"Schema User">
password=<"Schema User Password">
jdbcUrl="jdbc:oracle:thin:@<db host name>:<db port>:<schema name>/SID"
driverClass="oracle.jdbc.driver.OracleDriver"   maxPoolSize="100"
                                  minPoolSize="5"
             acquireIncrement="5"
numHelperThreads="20"
maxIdleTime="600"
maxIdleTimeExcessConnections="300"
debugUnreturnedConnectionStackTraces="true"
unreturnedConnectionTimeout="900" />
```

8. To add more <resource> entries, see the *AlertEnterprise Enterprise Guardian Installation Guide*.

2.1.12 Start the Server

1. Make sure that Active MQ is up and running and then start the Tomcat server.
2. Start the AlertEnterprise application using the address of the form http://<Server IP Address>:8080/AlertEnterprise.

   Note: 8080 is the default port on local host. If you want to change it, change it in the server.xml.

3. Log on to the application using username *admin* and password: *System@123*. You should be able to view the Home screen of the application.

2.1.13 Provisioning Configuration

For this build, the AlertEnterprise support team pre-configured AlertEnterprise Enterprise Guardian for provisioning. Configuring the provisioning functionality involves several steps to ensure that each connector is properly provisioning attributes. All steps for configuring provisioning are documented and delivered with the application in the **Help** tab. The parameters used during the configuration of different components are found here.

2.1.14 Creating System Connectors

1. Navigate to **Setup > Manual Configuration > Systems > System**.
2. Click **New** to create a new system.
3. Enter the following Definition:
   a. System Type – `Active Directory`
   b. Connector Name – `AD`
   c. Connector Description – `AD`
   d. Connector Long Description – `AD`
   e. Connector Type – `LDAP` (default)
4. Click **Next**.

5. Enter the following Parameters:
    a. HostName – `192.168.19.10`
    b. Port Number – `636` (use `389` if SSL is not configured yet)
    c. Service user Dn – `CN=AlertServiceAccount,CN=Users,DC=Acmefinancial,DC=com`
    d. Password – `Fsarm@nccoe1`
    e. Use SSL – `true` (use `false` if SSL is not configured yet)
    f. User Base DN – `OU=Operations,DC=Acmefinancial,DC=com`
    g. Group Base DN – `DC=Acmefinancial,DC=com`
    h. Object Class – `user`
    i. Is Primary – `Yes`
    j. LastModified Column role – `whenChanged`
    k. Last Modified User Column – `whenChanged`
6. Click **Next**.
7. Enter the following parameters:
    a. Application – `AlertAccess`
    b. Check the following boxes – `Provisioning, Role Management, Offline System, Allow Modify Role`
    c. Category – `production`
    d. Time Zone – `Eastern Standard Time`
8. Click **Next.**
9. Click **Save.**
10. Repeat Steps 1–9 to add the OpenLDAP and RACF connectors with the following parameters:
    OpenLDAP:
    a. System Type – `OpenLDAP Server`
    b. Connector Name – `OPENLDAP`
    c. Connector Description – `OpenLDAP`
    d. Connector Type – `OpenLDAP`
    e. HostName – `192.168.19.11`
    f. Port Number – `636` (use 389 if SSL is not configured yet)
    g. Service user Dn – `CN=Admin,DC=Acmefinancial,DC=com`
    h. Password – `Fsarm@nccoe1`
    i. Use SSL – `true` (use false if SSL is not configured yet)
    j. User Base DN – `OU=Operations,DC=Acmefinancial,DC=com`
    k. Group Base DN – `OU=Operations,DC=Acmefinancial,DC=com`
    l. Object Class – `inetOrgPerson`
    m. Group Object Class Name – `groupOfUniqueNames`
    n. Primay Connection – `Yes`
    o. LastModified Column role – `whenChanged`
    p. Last Modified User Column – `whenChanged`
    q. Member Attribute Name for Group – `uniqueMember`
    r. LDAP DnName – `cn`
    s. LDAP Account Control Column Name – `cn`
    t. User Password attributed – default
    u. Encode Password Required? – default
    v. LDAP Group Search Attributed – `cn`

w. userIdColumnName (Optional Parameter) - `cn`
x. Application – `AlertAccess`
y. Check the following boxes – `Provisioning, Role Management, Offline System, Allow Modify Role`
z. Category – `production`
aa. Time Zone – `Eastern Standard Time`

RACF:

a. System Type – `OpenLDAP Server`
b. Connector Name – `RACF_OPENLDAP`
c. Connector Description – `RACF_OpenLDAP`
d. Connector Type – `OpenLDAP`
e. HostName – `172.17.212.10`
f. Port Number – `636` (use 389 if SSL is not configured yet)
g. Service user Dn – `racfid=TSNI00,profiletype=user,sysplex=sysplex1`
h. Password – `Fsarm@nccoe1`
i. Use SSL – `true` (use false if SSL is not configured yet)
j. User Base DN – `profiletype=user,sysplex=sysplex1`
k. Group Base DN – `profiletype=user,sysplex=sysplex1`
l. Object Class – `racfUser`
m. Primay Connection – `Yes`
n. LDAP DnName – `racfId`
o. LDAP UserID Column Name – `racfId`
p. User Password attributed – default
q. Encode Password Required? – default
r. Ignore user check – `Yes`
s. isObjectClassExist – `No`
t. userIdColumnName (Optional Parameter) – `racfid`
u. isCnAttrExists (Optional Parameter) – `No`
v. Application – `AlertAccess`
w. Check the following boxes – `Provisioning, Role Management, Offline System, Allow Modify Role`
x. Time Zone – `Eastern Standard Time`

File Connector

a. System Type – `File Connector`
b. Connector Name – `FILE CONNECTOR`
c. Connector Type – `FileConnector`
d. User Folder Path – `C:\Program Files\User`
e. Role Folder Path – `C:\Program Files\Role`
f. User role Folder Path – `C:\Program Files\UserRole`
g. Column Header for User ID – `UserId`
h. Skip Provisioning – `Yes`
i. Application – `AlertAccess`
j. Check the following boxes – `Provisioning, Role Management`
k. Category – `Production`
l. Time Zone – `Eastern Standard Time`

Identity Store

a. System Type – `Database (JDBC J2EE)`
b. Connector Name – `IDENTITYSTORE`
c. Connector Type – `Database (JDBC J2EE)`
d. User Name – `admin`
e. Password – `System@123`
f. JNDI Name – `java:comp/env/jdbc/alntdb`
a. Application – `Alert Access`
b. Check the following boxes – `Provisioning, Role Manangement, Offline System, Identity Provider`
g. Category – `Production`
h. Time Zone – `Eastern Standard Time`

2.1.15 User Data Source

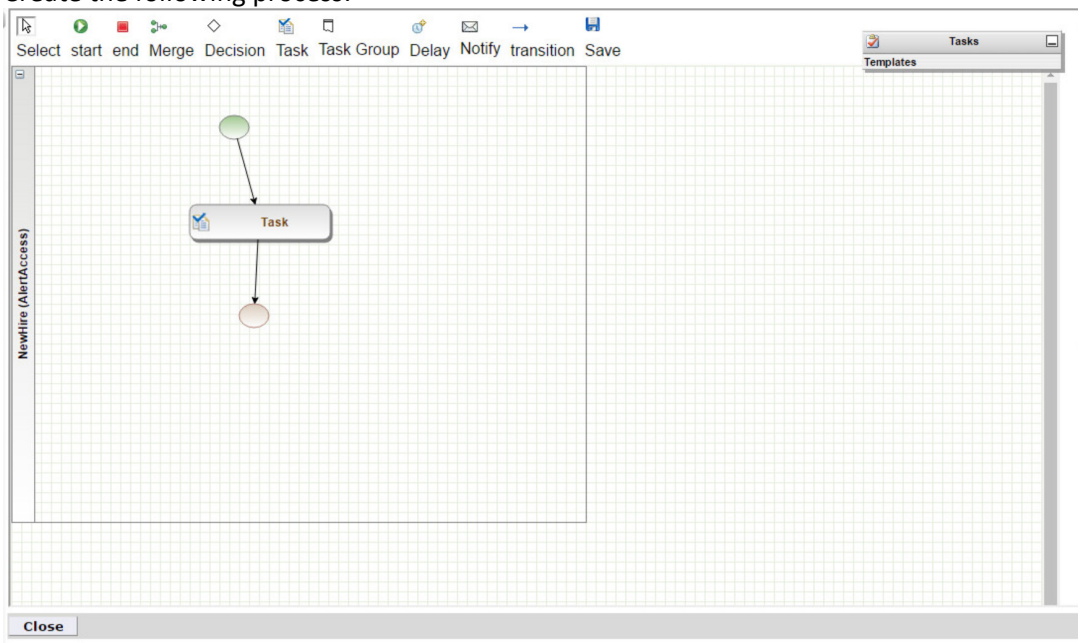
1. Navigate to **Setup>Manual Configuration>User Data>User Data Source.**
2. Click **New.** Create the following User Data Source:

System Type	Connector	Unique Key	Sequence	Mapping
Database (JDBC J2EE)	IDENTITYSTORE	UserId	1	1) UserId – IDENTITYSTORE – UserId 2) FirstName – IDENTITYSTORE – FirstName 3) LastName – IDENTITYSTORE – LastName 4) ValidFrom – IDENTITYSTORE – ValidFrom 5) ValidTo – IDENTITYSTORE – ValidTo

2.1.16 Process Designer

1. Navigate to **Setup>Manual Configuration>Process Engine>Process Designer.**
2. Click **New.**
3. Enter `New Hire` as Process Name and `Alert Access` as Rule Type. Click **Next.**

4. Create the following process:



2.1.17 Policies

1. Navigate to **Setup>Manual Configuration>Policy Engine>Policies.**
2. Click **New.** Create the following policies:

Policy Name	Rule Name	Priority	Active	Attribute Name	Value
OpenLDAP prov Action	OpenLDAP prov Action	0	Yes	System ProvAction	Change_Roles
Termination-shell update	Termination-shell update	0	Yes	loginShell	disable

2.1.18 Rules

1. Navigate to **Setup>Manual Configuration>Policy Engine>Rules.**
2. Click **New.** Create the following rules:

Rule Name	Entity Type	Rule Type	Description	Applicable To	Attributes	Condition
Survey Rule	Workflow	Survey	Survey Rule	Initiator	AND	
NewHire	Workflow	AlertAccess	NewHire	Initiator	AND Request Category	= Change Access
NewHireSuggestDefault	Workflow	AlertAccess	NewHireDefault	Suggest/Default	AND Request Category	1) =NewHire 2) =Change-Acces 3) =Rehire
Role Assignement	Workflow	AlertAccess	Role Assign	Policy	AND Role:Alias	Any Value
OpenLDAP prov Action	Workflow	AlertAccess	OpenLDAP provisioning action	Policy	AND Request Category; System Multi Select	1) =Termination and =OpenLDAP 2) =Rehire and =OpenLDAP
Termination-shell update	Workflow	AlertAccess	Terminate shell update	Policy	AND Request Category	=Termination

2.1.18.1 Suggest/Default Access

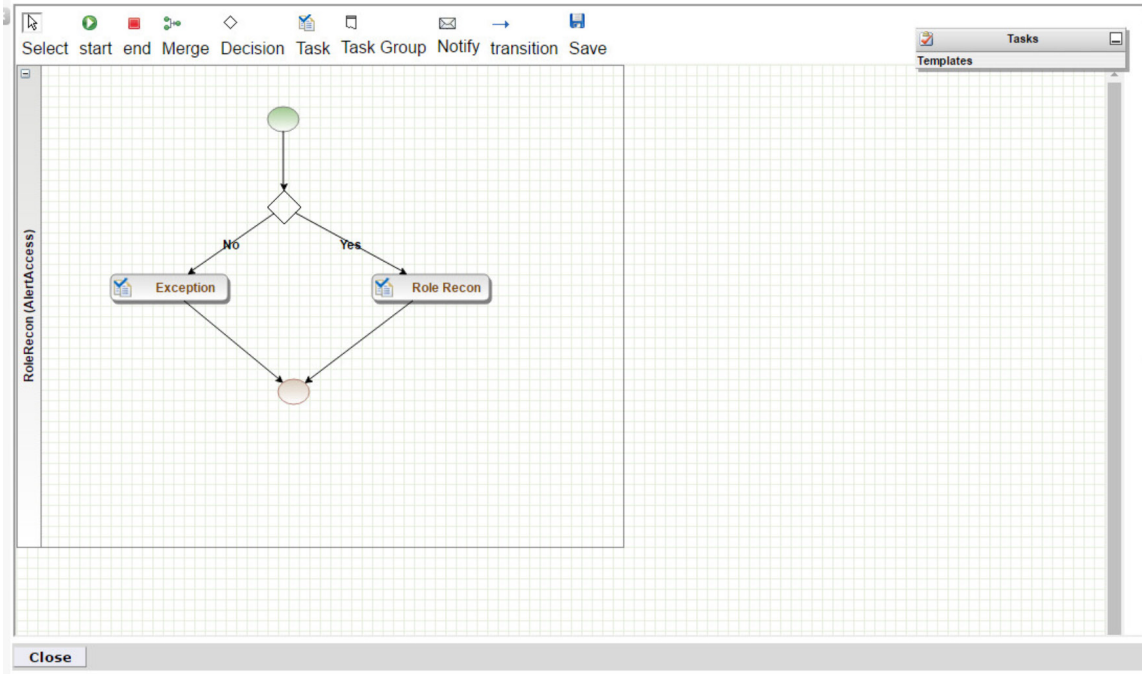
1. Navigate to **Setup>Manual Configuration>Policy Engine>Suggest/Default Access.**
2. Click **New.** Create the following criteria:

Name	Type	Condition	Search By	Resources	Attributes
NewHire	Default	NewHireSuggestDefault	Systems	OpenLDAP, AD, RACF_OPENLDAP	
DefaultRole-Assignment	Default	NewHireSuggestDefault	Role Attributes		Alias
123	Defaul	NewHireSuggestDefault	Role Attributes		RoleDescription

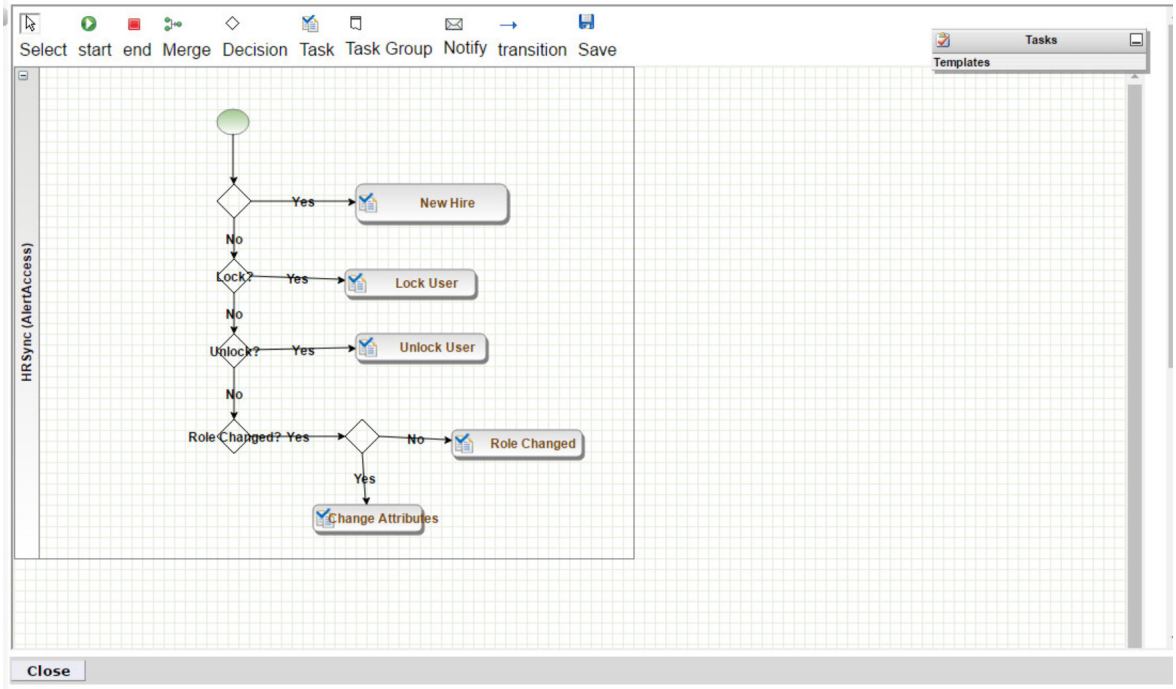
2.1.19 Policy Designer

1. Navigate to **Setup>Manual Configuration>Policy Engine>Policy Designer.**
2. Click **New.**
3. Enter `RoleRecon` as the **Name** and `Alert Access` as the **Rule Type**.

4. Create the following policy:



5. Repeat Steps 1-4 for with HRSync as the **Name** and the following policy:



2.1.19.1 Rule Action Handlers

1. Navigate to **Setup>Manual Configuration>Policy Engine>Rule Action Handler.**
2. Click **Create.** Create the following action handlers:

Action Handler Name	Workflow	Task Type	Value	Priority	Update Identity Info	Evaluate Enter-prises Role
Termination	AlertAccess	Recon Create Request	Termination	0	Yes	No
Recon Excep-tion	AlertRecon	Recon Exception Record		0		
NewHire	AlertAccess	Recon Create Request	NewHire	0	Yes	No
Rehire	AlertAccess	Recon Create Request	Rehire	0	Yes	No
UpdateRepo	AlertAccess	Update Identity Info	Yes	0	Yes	No
Role recon	AlertRecon	Recon Create role in Repo		0		
ChangeAc-cess	AlertAccess	Recon Create Request	ChangeAccess	0	Yes	No
ChangeUser	AlertAccess	Recon Create Request	ChangeUser	0	Yes	No
Attribute Change	AlertAccess	Recon Create Request	Attribute Change	0	Yes	No

2.1.19.2 Job Triggers

1. Navigate to **Setup>Manual Configuration>Job Scheduler>Triggers.**
2. Click **Create.** Create the following trigger:

Name	HRSync
Description	HRSync
Type	Reconciliation
Batch Size	100
Number of Attempts	3
Policy Designer for Users	HRSync
Policy Designer for roles	RoleRecon
System:Reconciliation From	FILE CONNECTOR
Reconciliation System:	FILE CONNECTOR
Field Mapping Group	HR Sync
Process Deleted Option for Full Reconciliation	User Role
Process Deleted Option for Incremental Reconciliation	User Role

2.1.20 Triggers Field Map

598 1. Navigate to **Setup>Manual Configuration>Job Scheduler>Triggers Field Map.**
599 2. Click **Create.** Create the following field map group:
600

Group Name	Type
HR Sync	Reconciliation

601 ### 2.1.21 Form Customization

602 1. Navigate to **Setup>Manual Configuration>Form Customization>Attributes.**
603 2. Click **Create.** Create the following attributes:

Name/Label	Attribute Type	Visible	Mandatory	Data Type	Field Type	Check Boxes
ADUserId	Custom	No	No	String	Textbox	Provisioning
LDAPUserId	Custom	No	No	String	Textbox	Provisioning
ADuserName	Custom	No	No	String	Textbox	Provisioning
LDAPuserName	Custom	No	No	String	Textbox	Provisioning
FirstName	Standard	Yes	Yes	String	Textbox	Provisioning
EmployeeNo	Custom	No	No	String	Textbox	Provisioning
BaseDN	Custom	No	No	String	Textbox	Provisioning
L	Custom	No	No	String	Textbox	Provisioning
Pager	Standard	Yes	Yes	String	Textbox	Provisioning
Initials	Standard	Yes	No	String	Textbox	Provisioning
Racfid	Custom	No	No	String	Textbox	Provisioning
Racfprogrammername	Custom	No	No	String	Textbox	Provisioning
Racfworkattrusername	Custom	No	No	String	Textbox	Provisioning
Racfaddressline1	Custom	No	No	String	Textbox	Provisioning
Racfaddressline4	Custom	No	No	String	Texbox	Provisioning

604 *Note:* This list is not exhaustive. The application is deployed with several attributes preconfigured.

605 ### 2.1.22 User Field Mapping

606 1. Navigate to **Setup>Manual Configuration>Identity & Access>User Field Mapping.**
607 2. Select **Identity** from the drop-down menu. Click **Go**.
608 3. Click **Create New**.
609 4. Create the following field mappings:

Custom Field	Visible in List	isSearchable	Column Location
UserId	Yes	Yes	1
ValidFrom	No	No	2
ValidTo	No	No	3
FirstName	Yes	Yes	4
LastName	Yes	Yes	5
Alias	No	No	6

Email	No	No	7
ManagerId	No	No	8
Department	No	No	9
JobTitle	No	No	10
CompanyName	No	No	11
ManagerName	No	No	12
FullName	No	No	13
Mobile	No	No	14
User Base Dn	No	No	15
ADUserId	No	No	16
LDAPUserId	No	No	17
ADuserName	No	No	18
LDAPuserName	No	No	19
EmployeeNo	No	No	20
Initials	No	No	21
Pager	No	No	22
L	No	No	23
Racfid	No	No	24
Racfprogrammername	No	No	25
Racfworkattrusername	No	No	26
Racfaddressline1	No	No	27
Racfaddressline4	No	No	28

2.1.23 Provisioning Mapping

1. Navigate to **Setup>Manual Configuration>Identity & Access>Provisioning>Provisioning Mapping.**
2. Select the connector and click **Configure** for the following connectors:

IDENTITYSTORE

Database Attribute Name	Mandatory	AlertEnterprise Attribute Name	Default Value	Editable	Visible	Validation Flag	isUser-Id attribute
FullName	No	FullName	$<FirstName> $<LastName>	No	No	No	No

OPENLDAP

Database Attribute Name	Mandatory	AlertEnterprise Attribute Name	Default Value	Editable	Visible	Validation Flag	isUser-Id attribute
Cn	No	LDAPUserId		Yes	Yes	No	Yes
Sn	No	LastName		Yes	Yes	No	No
givenName	No	FirstName		Yes	Yes	No	No
UserBaseDn	No	BaseDn		Yes	Yes	No	No

uidNumber	No	uidNumber	1	Yes	Yes	No	No
gidNumber	No	gidNumber	1	Yes	Yes	No	No
homeDirectory	No	Homedirectory		Yes	Yes	No	No
objectClass	No	UserObjectClass	inetOrgPerson| organizationalPerson| Person|Top| PosixAccount			No	No
Mail	No	Email		Yes	Yes	No	No
userPassword	No	Password		Yes	Yes	No	No
employeeNumber	No	EmployeeNo		Yes	Yes	No	No
Mobile	No	Mobile		No	No	No	No
DepartmentNumber	No	Department		No	No	No	No
Title	No	JobTitle		No	No	No	No
O	No	CompanyName		No	No	No	No
loginShell	No	loginShell		No	No	No	No
Uid	No	LDAPUserId		Yes	Yes	No	Yes
L	No	L		No	No	No	no

616 **AD**

Directory Attribute Name	Mandatory	AlertEnterprise Attribute Name	Default Value	Editable	Visible	Validation Flag	isUser-Id attribute
sAMAccountName	No	ADUserId		Yes	Yes	No	Yes
Sn	No	LastName		Yes	Yes	No	No
givenName	No	FirstName		Yes	Yes	No	No
accountExpires	No	ValidTo		Yes	Yes	No	No
UserBaseDn	No	User Base Dn		Yes	Yes	No	No
unicodePwd	No	Password	System@123	Yes	Yes	No	No
displayName	No	DispalyName	$<LastName>, $<FirstName>	Yes	Yes	No	No
Mail	No	Email		Yes	Yes	No	No
employeeNumber	No	EmployeeNo		No	No	No	No
Mobile	No	Mobile		No	No	No	No
Department	No	Department		No	No	No	No
userPrincipalName	No	NISTEmptyDN	$<UserID>@AcmeFinancial.com	No	No	No	No
Title	No	JobTitle		No	No	No	No
Company	No	CompanyName		No	No	No	No
userAccountControl	No	UserAccountControl	512	No	No	No	No
Pager	No	Pager		No	No	No	No
Initials	No	Initials		No	No	No	no

617 **RACF_OPENLDAP**

Directory Attribute Name	Mandatory	AlertEnterprise Attribute Name	Default Value	Editable	Visible	Validation Flag	isUser-Id attribute
Racfid	Yes	Racfid		No	No	No	Yes
Racfworkattrusername	No	Racfworkattrusername		No	No	No	No
UserBaseDn	Yes	homeDirectory	profiletype=user, sysplex=sysplex1	No	No	No	No
objectClass	No	UserObjectClass	racfUser	No	No	No	No

Racfprogrammername	No	Racfprogrammername		No	No	No	No
Racfaddressline1	No	Racfaddressline1		No	No	No	No
Racfaddressline4	No	Racfaddressline4		No	No	No	No

2.1.24 External Provisioning Attributes

1. Navigate to **Setup>Manual Configuration>Identity & Access>Provisioning>External Provisioning Attributes.**
2. Select the connector and click **Configure** for the following connectors:

OPENLDAP

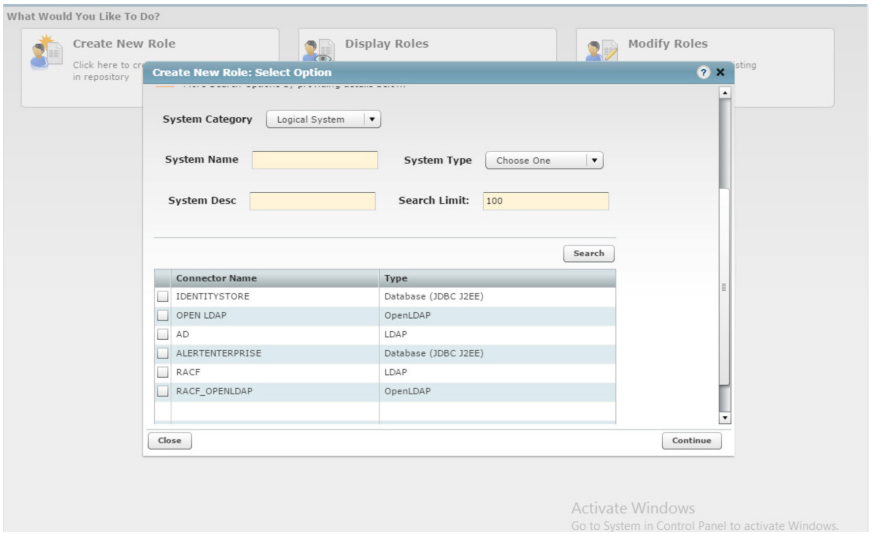
Name	Description
loginShell	loginShell

RACF_OPENLDAP

Name	Description
Racfid	Racfid
Racfworkattrusername	Racfworkattrusername
UserBaseDn	UserBaseDn
objectClass	objectClass
Racfprogrammername	Racfprogrammername
Racfaddressline1	Racfaddressline1
Racfaddressline4	Racfaddressline4

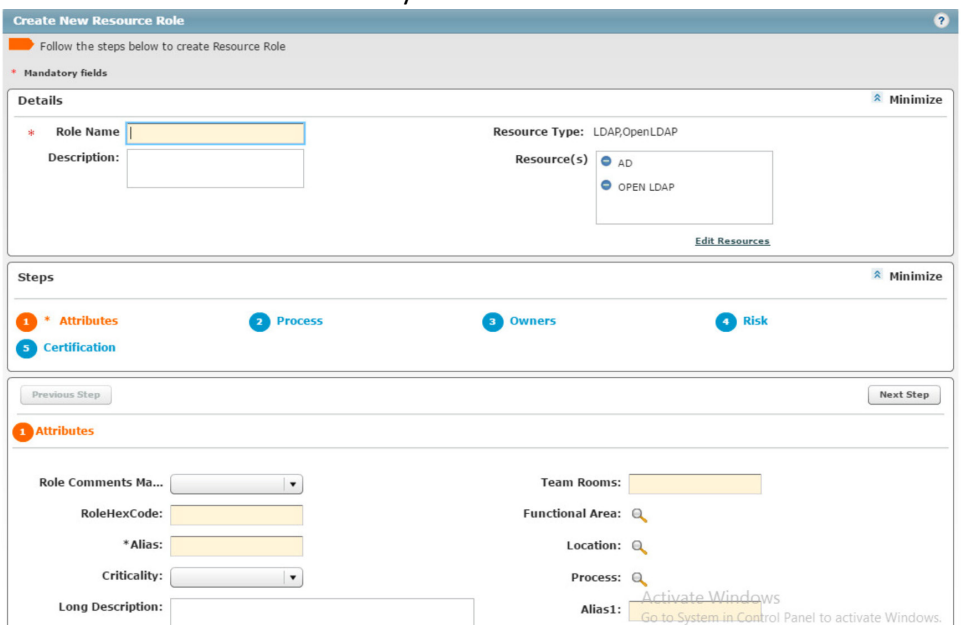
2.1.25 Role Repository

1. Navigate to **Setup>Manual Configuration>Role Repository**.
2. Click **Create New Role** to begin.

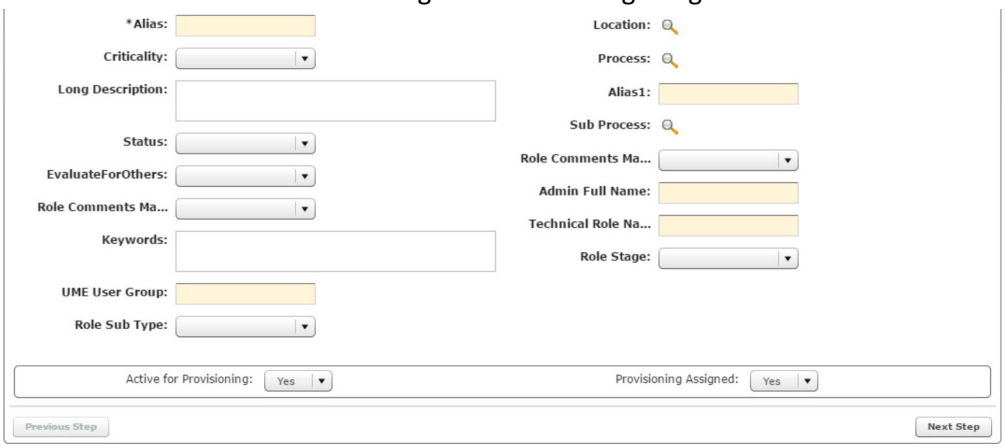


3. Select **Create New Role** from Start.
4. Click **Search** to load the connector names. Select the **OpenLDAP** and **AD** connectors.
5. Click **Continue.**

6. Enter a **Role Name** and **Alias**. They must be identical.



7. Select **Yes** for Active for Provisioning and Provisioning Assigned.



8. Create the following roles in the repository:

Role Name	Resource(s)
Accounting Manager	AD, OpenLDAP
Branch Manager	AD, OpenLDAP
Financial Analyst	AD, OpenLDAP
Financial Manager	AD, OpenLDAP
Loan Officer	AD, OpenLDAP
Operations Manager	AD, OpenLDAP
Security Analyst	AD, OpenLDAP
Systems Admin	AD, OpenLDAP
Teller	AD, OpenLDAP
VM Admin	AD, OpenLDAP

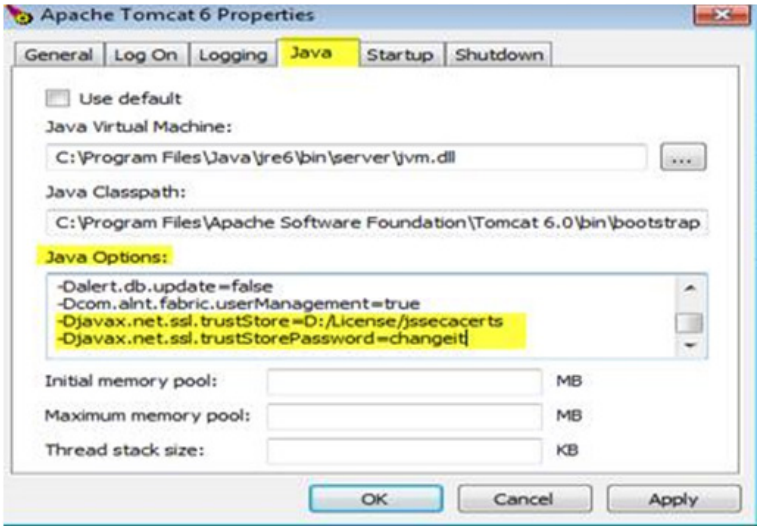
2.1.26 Enabling SSL

To better secure LDAP communications between AlertEnterprise Enterprise Guardian and the directory servers, we have configured such communications to use SSL encryption. Specifically, the LDAPS protocol has been configured. The steps to configure LDAPS for each connection to a directory server are as follows:

1. Create a *D:\cert\folder* on your system.
2. Place certificate jar file inside that folder.
3. Open the command prompt in administrator mode and perform the command:
   `cd D:\cert\`
4. Download certificate from directory server using the following command:
   `java -cp ALNTADCertUtil.jar com.alnt.ADCertInstaller`
   `<IP_Address_Of_Directory_Server>`**`:636`**

   This creates the jssecacerts file in **`D:\cert\`** folder.
5. Add the following D parameters in `<Tomcat Installation Folder>/bin/Tomact6w`
   `-Djavax.net.ssl.trustStore=D:/License/jssecacerts`

   `-Djavax.net.ssl.trustStorePassword=changeit`



6. Copy jssecacerts to D:/License (create this folder if it does not exist) and restart Tomcat.
7. Switch connection back to 636 port and set SSL as true from false.

2.2 HyTrust Cloud Control

HyTrust CloudControl provides a variety of security and policy enhancements to the virtual infrastructure without impacting the GUI tha vSphere, NSX and ESXi admins already know and use. HyTrust CloudControl mediates the actions taken by virtual infrastructure administrators using familiar interfaces. Approved actions are allowed, disapproved actions are blocked and additional approval workflow is enabled.

2.2.1 How Its Used

HyTrust CloudControl (HTCC) is used as a centralized point of control for access management within the virtual infrastructure of this example implementation.

2.2.2 Virtual Machine Configuration

HTCC uses one ESXi host and two virtual machines for its infrastructure. One virtual machine is the HTCC appliance. This virtual machine is delivered as an .OVF file from the HyTrust support site. The other virtual machine is a VCenter server, which is installed as a virtual machine within the ESXi host.

Note: The ESX host and HTCC Virtual Machine requirements depend on the specific load of a protected virtual environment. See the HTCC installation guide for a complete list of system requirements.

VCenter Server:

- Windows Server 2012 R2
- 2 CPU core
- 16GB of RAM (memory)
- 1 NIC
- 60GB of storage

HTCC:

- CentOS 4/5/6/7 (64-bit)
- 4 CPU core
- 16GB of RAM (memory)
- 1 NIC
- 70GB of storage

Network Configuration (VCenter Server)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.20.6
Netmask: 255.255.255.0
Gateway: 192.168.20.1
DNS Name Servers: 192.168.19.10
DNS-Search Domains: acmefinancial.com

Network Configuration (HTCC)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.20.11
Netmask: 255.255.255.0
Gateway: 192.168.20.1
DNS Name Servers 192.168.19.10
DNS-Search Domains: acmefinancial.com

2.2.3 Installing Vcenter Server

Install Vcenter Sever 6.0 according to the VMware documentation found here.

2.2.4 Configuring Vcenter Server

Vcenter server is configured with 1 host and 1 data center.

ESXi Host:

1. VMware ESXi, 6.0.0
2. Dell PowerEdge R620
3. 20 CPUs x 2.8 GHz
4. 23,478 mb / 262,098 mb
5. 8 Physical Adapters

2.2.5 Deploying HTCC

Before installing the HTCC appliance, the following conditions should be in place:

- Virtual infrastructure, consisting of installed vCenter Servers and, optionally, ESX hosts.
- Network connectivity and access to the HTCC host machine.
- The HTCC installation requires an ESX host with at least one dedicated network interface (using VLANs).
- For Directory Service mode authentication, setup of Microsoft Active Directory (AD) with an AD Service Account and the recommended HyTrust security groups, as described in the *HyTrust CloudControl Administration Guide*.
- Services used by virtual infrastructure clients should be routable from the appropriate interface.

See the HTCC installation guide for a step-by-step guide on deploying the HTCC appliance. The installation guide is available on request.

2.2.6 Configuring HTCC

The HTCC Management network interface (eth0) must be manually configured before you can access the HTCC Management Console.

Configure the HTCC Management network interface:

1. At the vSphere Client console window, log in as the user *ascadminuser* with the password Pa$$w0rd123!.
2. You are prompted to assign a new password to the local HTCC administrator account (*ascadminuser*). Be sure to keep your new password in a safe and secure place.
3. Start the setup procedure. At the prompt, type: `setup`
4. Manually assign a static IP address to the management network interface (eth0) and set the subnet mask, gateway, and DNS server addresses.

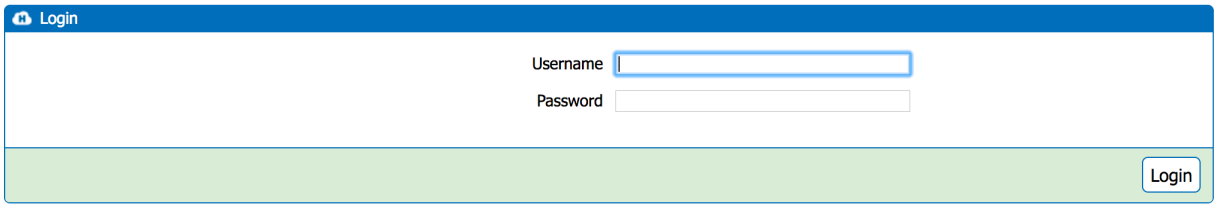
5. Save by typing: `y`
6. Log out after network settings have been saved. This build is configured with the following settings:

```
Last login: Wed Apr  5 15:13:50 on ttys001
[MM229136-PC:~ dwynne$ ssh ascadminuser@10.33.50.38
[ascadminuser@10.33.50.38's password:
Last login: Wed Apr  5 19:20:39 2017 from 10.97.67.143
[[hytrust:standalone ~]$ setup

CloudControl Setup - HyTrust CloudControl - 4.6.2.46611

Please specify network settings for the Connection 1 (eth0) interface

The appliance is configured with the following settings:

        IP: 192.168.20.11
   Netmask: 255.255.255.0
   Gateway: 192.168.20.1
 DNS Server: 192.168.19.10
```

The HTCC web-based management console is used to customize the HTCC settings. When accessing HTCC for the first time, you must use the IP address in the URL. For example:
`https://<ipaddress>/asc`

1. Enter the IP address of the HTCC Management network interface.
2. Manually allow the security exception.

The login screen appears.

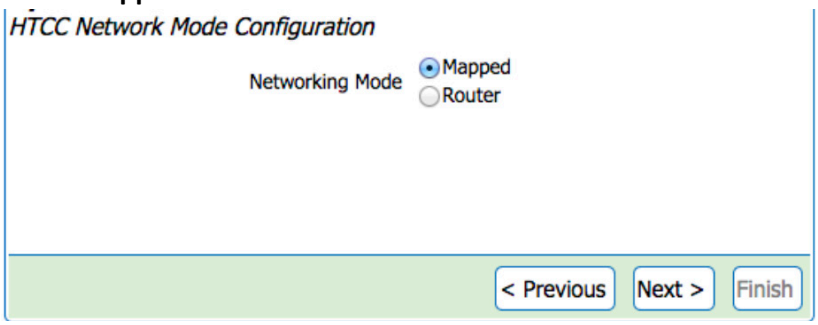


Once logged in, you can complete the initial setup and configuration. Here is an overview of the initial setup and configuration steps. The detailed steps can be found in the HTCC installation guide, which is available on request.

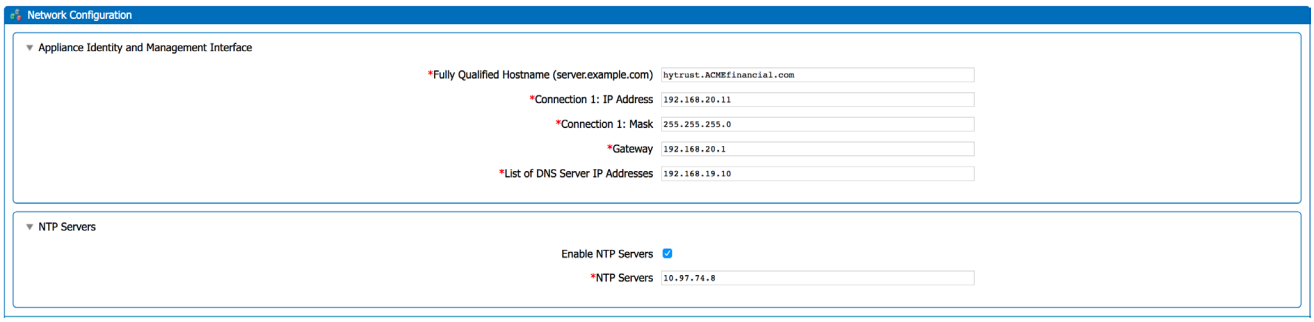
1. Accept the end-user license agreement.
2. If applicable, install a license.
3. Complete the **HTCC Installation Wizard** based on your selected networking mode.
4. Perform post-installation setup.

HTCC Installation Wizard:

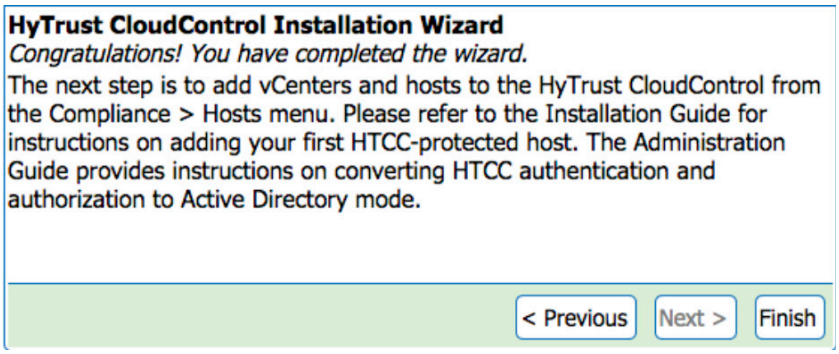
1. Select **Mapped** as the HTCC Network Mode



2. Specify the network information on the Network Configuration page. This build is configured as follows:

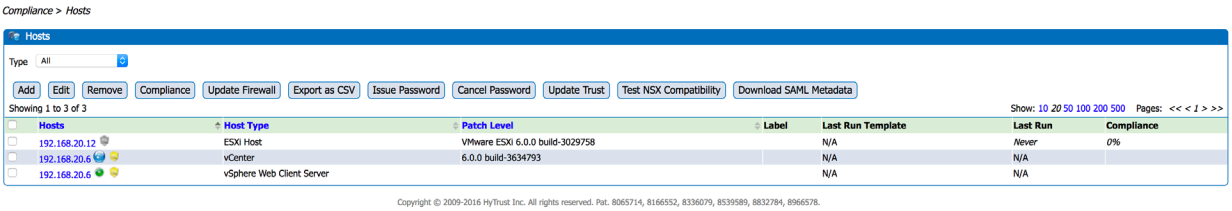


3. Click **Next** and select **Finish.**

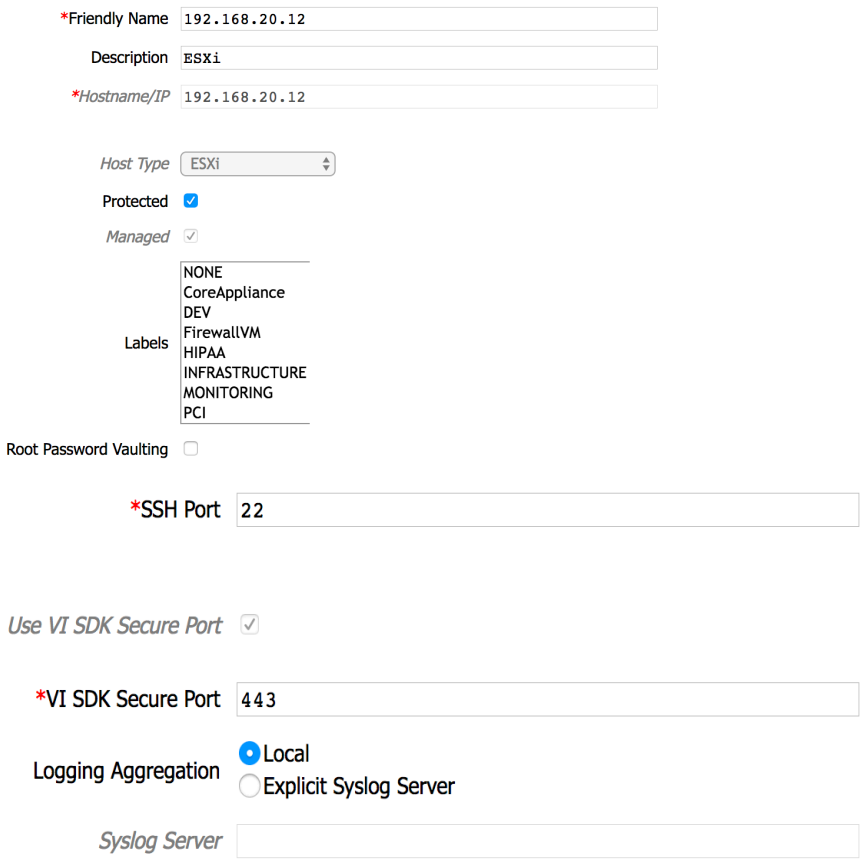


Add VCenter and Hosts to the HTCC:

In this build, three managed hosts are added. The three hosts are ESXi, Vcenter, and Vcenter Web Client Server. For the full list of options for the host and detailed steps of adding a host, see the HTCC installation guide. The configurations of each added host are as follows:



ESXi:



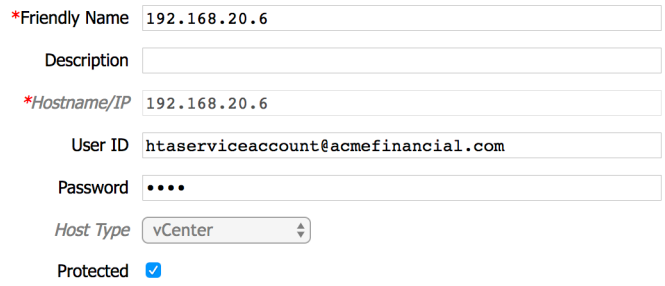
763

764

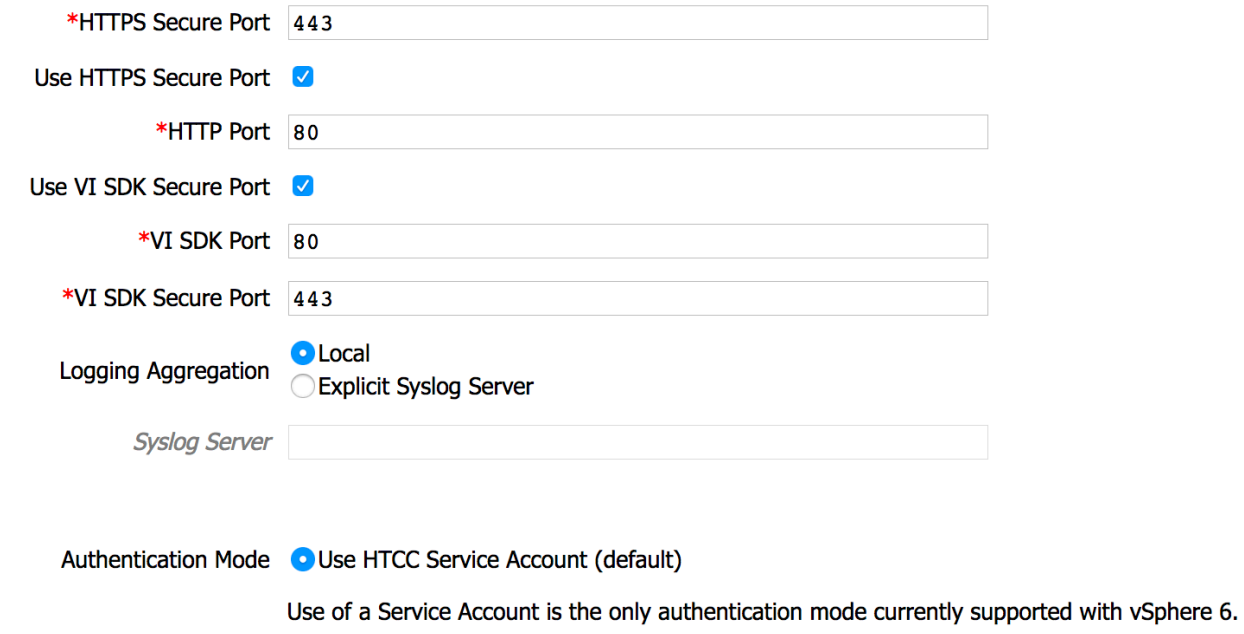
765 *Note:* Ensure that each host is protected.

766

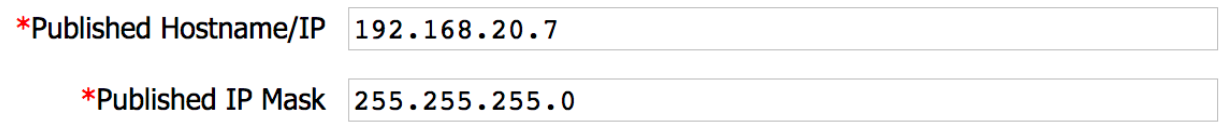
767 vCenter:



768



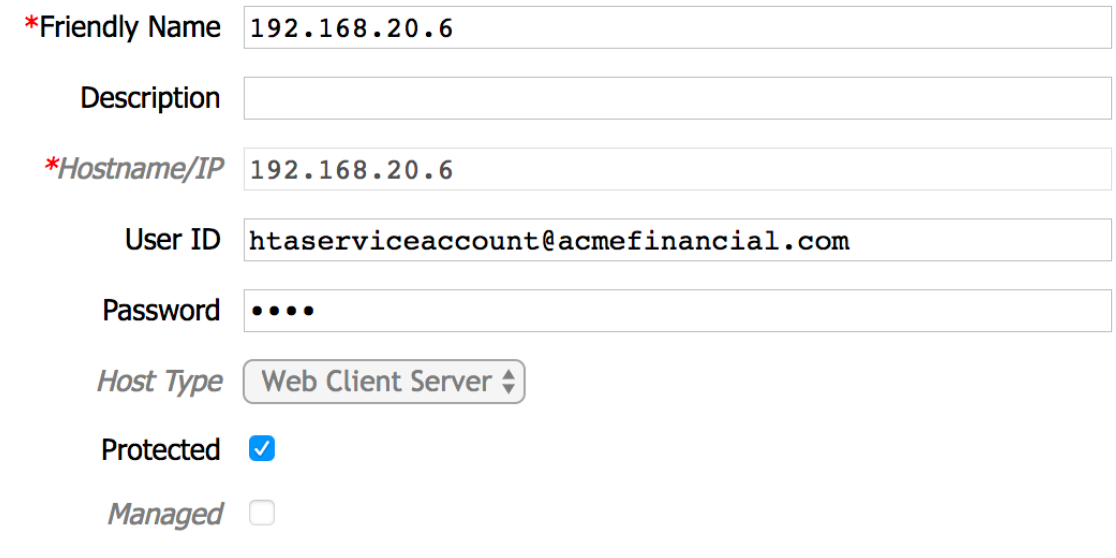
769



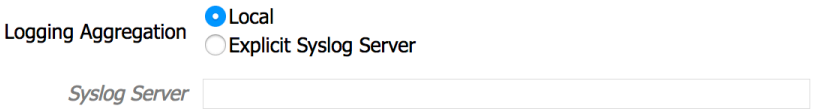
770

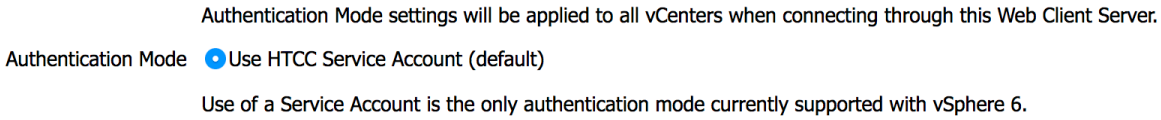
771 *Note:* The htaserviceaccount must be created in Active Directory first. See Integrating with Active
772 Directory.

773 vSphere Web Client Server:

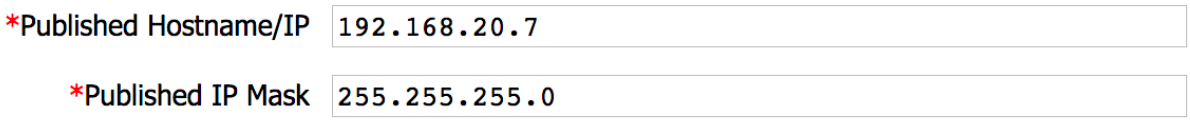


774





775



776

777 2.2.7 Integrating With Active Directory

778 In this build, HTCC is integrated with Active Directory. Users who have access to the virtual environment
779 have accounts in AD and are a part of the *'hytrust users'* group.

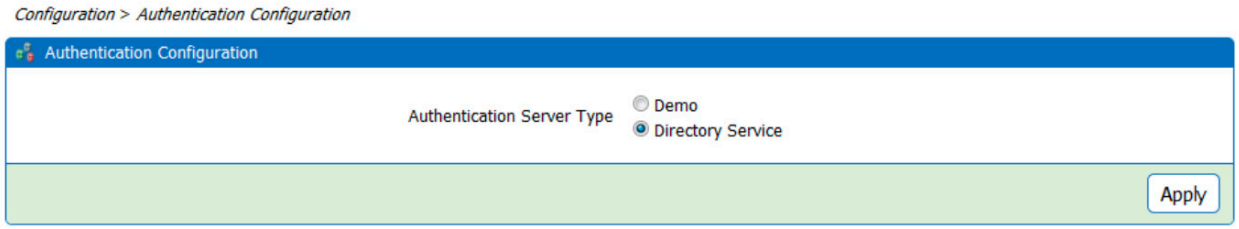
780 First, you must create a service account in Active Directory with the following permissions. In this build,
781 the *htaserviceaccount* is created.

782 - Domain object: *Read memberOf*
783 - User object: attributes *memberOf* and *distinguishedName*
784 - Group object: attributes *member*, *memberOf*, and *distinguishedName*

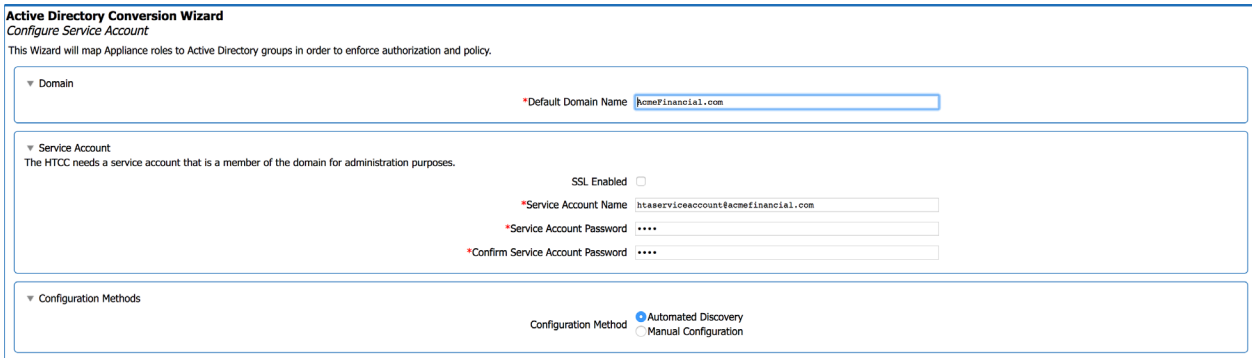
785 To convert HTCC to Directory Service mode:

786 1. Open the Authentication Configuration page (**Configuration > Authentication**).

2. Select the **Directory Service** radio button and click **Apply**.

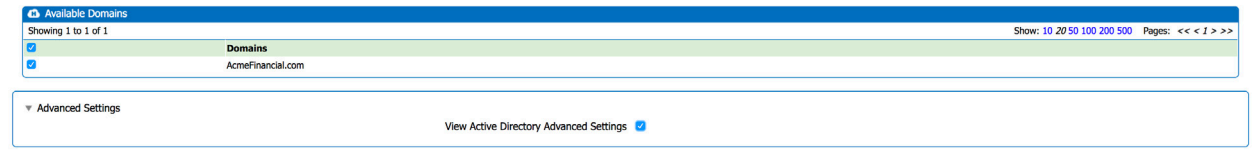


The Active Directory Conversion Wizard opens, which guides you through the steps to connect HTCC to your directory service. The first page is the Configure Service Account page.

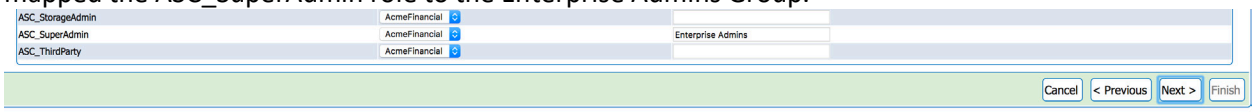


3. Use the Service Account panel to specify the AD HTCC service account information. Select **Automated Discovery**. Click **Next.**

Check **View Active Directory Advanced Settings** to view advanced settings. Otherwise, select **Next.**



The Rule Conversion page appears where you can map HTCC roles to AD groups. For this build, we mapped the ASC_SuperAdmin role to the Enterprise Admins Group.



Note: At a minimum, one Active Directory security group (e.g., SuperAdmin) must be mapped to HTCC ASC_SuperAdmin role for AD conversion to be successful.

4. Click **Next**.

A summary page appears confirming the AD settings. Review the information to make sure the **Domain Controllers**, **Rule Conversion**, and **Service Account** settings are accurate.

5. Click **Finish** to convert HTCC to Directory Service mode.

Perform the following steps to create the HTCC security groups in AD:

1. Create a security group for each HTCC you choose. For this build, two groups called '*Hytrust Users'* and '*Hytrust Users 2'* are created.
2. For each group, assign the Group scope to *Global* and the Group type to *Security*.

For additional configuration options for integrating with Active Directory. see the HTCC Administration Guide, which is available on request.

2.2.8 Creating and Deploying Access Policies

Before creating and deploying access policies on a virtual infrastructure, confirm that HTCC is protecting the vCenter Server and all the imported hosts. See the *HyTrust CloudControl Installation Guide* for assistance in importing a vCenter Server, adding a host, or protecting these resources.

After importing a vCenter Server protected host, HTCC adds the vCenter Server object structure to a new draft policy and deploys it automatically.

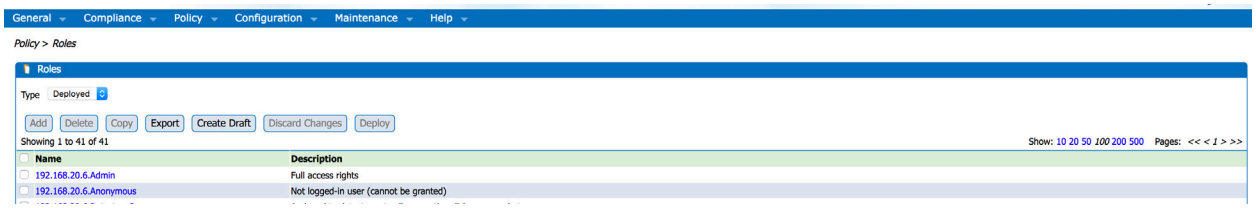
Any time a new virtual machine is created or a new host is added, the new object is automatically added to the HTCC policy and the deployed policy is enforced on the new object. To view the current policy, navigate to **Policy>Resources.** The *Deployed* policy is the policy that is currently in effect.

To make a change in the deployed policy, such as adding a new rule to a protected host, follow these steps:

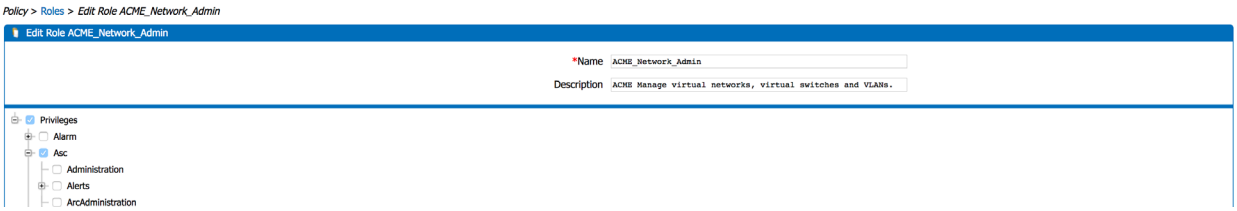
1. Open any **Policy** page.
2. Click the **Create Draft** button. This copies the "Deployed" policy to a "Draft" policy.
3. Make your desired changes to the Draft policy using the various policy pages.
4. Click the **Deploy** button to replace the current Deployed policy with the Draft policy.

For this build, two roles are created called **ACME_Network_Admin** and **ACME_Systems_Admin**. To create the rules and roles used to demonstrate the access rights management capability, follow these steps:

1. Navigate to **Policy>Roles.**
2. Select **Create Draft.**



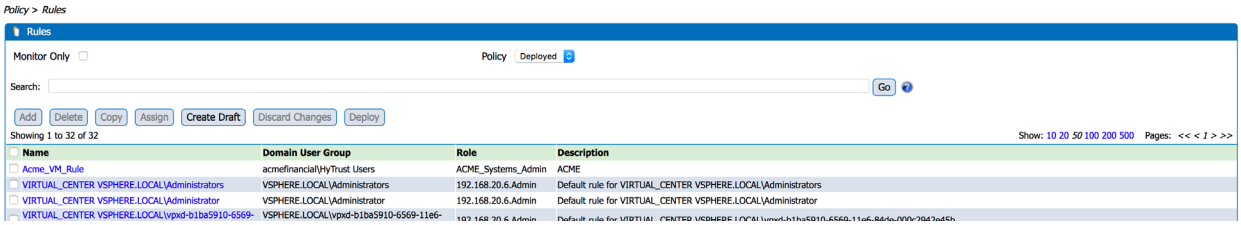
3. Select **Add.** First, create the network admin role. Then, name the role and provide a description.



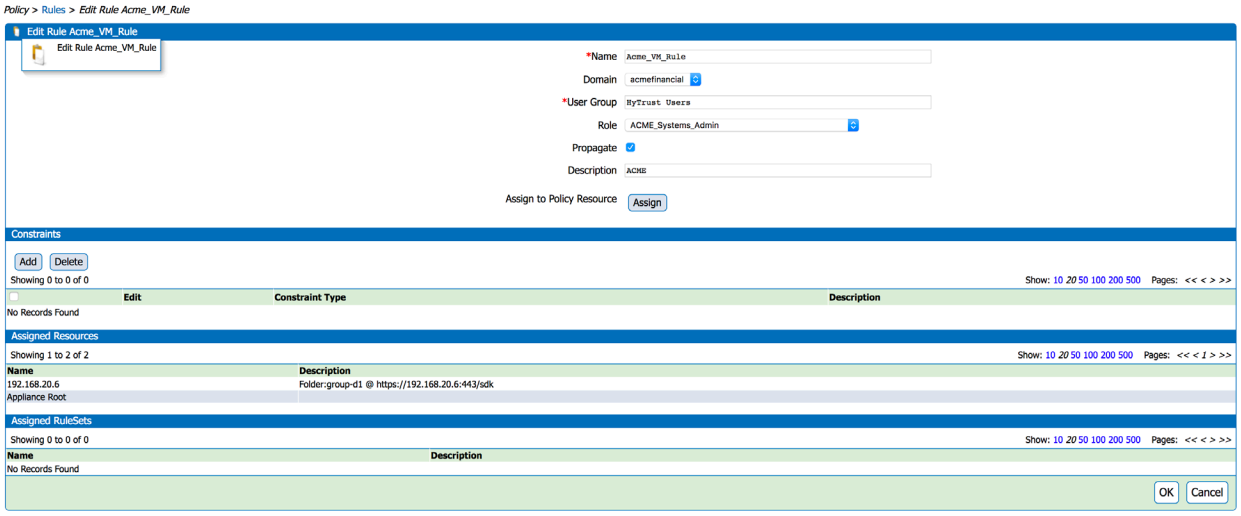
4. Select all of the following permissions:
    a. **Asc>NxOsConfig, NxOsShow, NxOsXmlApi,ssh,storage**
    b. **DVPortgroup>Entire List** (*Note:* This configuration item is deprecated in versions 5.1 and above of the product.)
    c. **DVSwitch>Entire List**
    d. **DataCenter>IpPoolConfig,IpPoolQueryAllocations,IpPoolReleaseIp**
    e. **Global>CancelTask,LogEvent**
    f. **Host>Config>AdvancedConfig,NetService,Network,PciPassthru**
    g. **Network>Assign,Delete,Router**
    h. **Resource>Delete**
    i. **System>Entire List**
    j. **Task>Entire List**
    k. **VirtualMachine>Config>ManagedBy,MultiActions**
5. Press **OK.**
6. Press **Deploy.**
7. Repeat Steps 2–6 to create the system admin role, but with the following permissions selected:
    a. **Global>CancelTask,LogEvent**
    b. **System>Entire List**
    c. **Task>Entire List**
    d. **VApp>Entire List**
    e. **VirtualMachine>Entire List**

Next, you must create the rules that will apply the roles to the host. First, create the rule for the system admins role, assigning it to the '*HyTrust Users'* AD group.

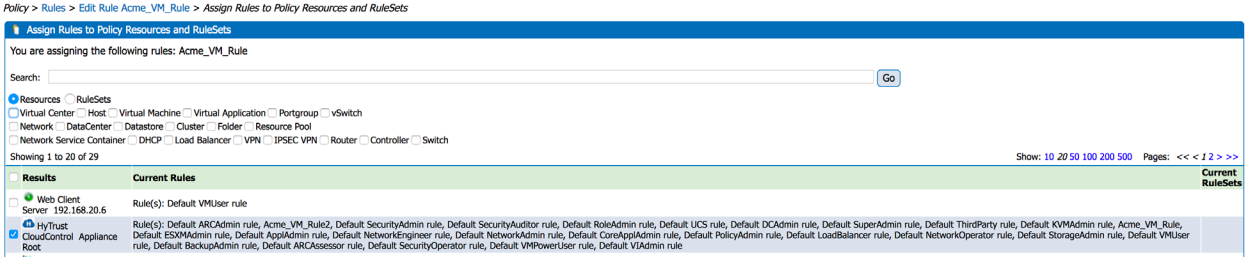
8. Navigate to **Policy>Rules.**
9. Select **Create Draft.**



10. Select **Add.** Name the rule and type in the user group created in Active Directory.



11. Select **Assign.**
12. Check the **HyTrust CloudControl Appliance Root** radio button.

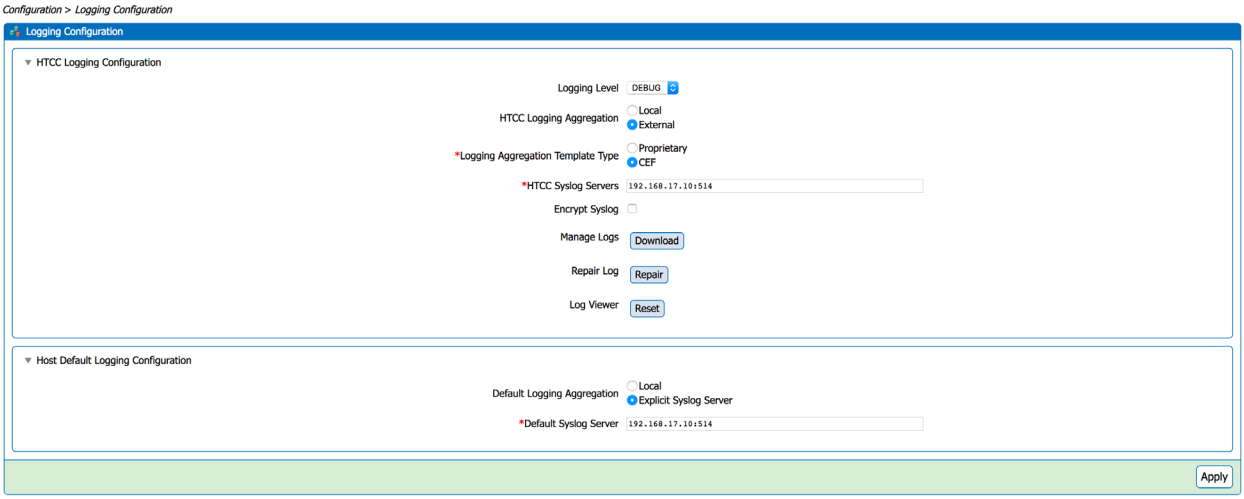


13. Select **OK.**
14. Select **OK.**
15. Select **Deploy.**
16. Repeat Steps 1–9 to create a rule for the network admins role, assigning it to the *'Hytrust Users 2'* active directory group.

2.2.9 Configure Logging

1. Select **Configuration > Logging.**
2. Select the **DEBUG** logging level.
3. Select **External.**
4. Select **CEF.**

5. Enter the IP address of the Splunk server, specify port 514.



6. Select **Explicit Syslog Server.**
7. Enter the IP address of the Splunk server, specify port 514.
8. Select **Apply.**

2.3 Microsoft Active Directory

An LDAP directory service that stores user account and attribute information.

2.3.1 How It's Used

Microsoft AD acts as one of the user identity management repositories in the example solution. AD can provision and de-provision user identities; the creation, modification, and deletion of subject attributes; and the provisioning and de-provisioning of subject attributes to specific user identities. Administration of user identity and attribute provisioning is controlled by AlertEnterprise Enterprise Guardian. AD is also used for its logging and auditing of user identity and attribute provisioning administration.

2.3.2 Virtual Machine Configuration

The AD virtual machine is configured as follows:

- 1 CPU Core
- 4GB RAM
- 84GB HDD
- 2 Network Adapters

Network Configuration (Interface 1)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.19.10
Netmask: 255.255.255.0
Gateway: 192.168.19.1

DNS Name Servers: 192.168.19.10
DNS-Search Domains: AcmeFinancial.com

2.3.3 Installing AD

Install a new Windows server 2012 R2 Active Directory Forest:

https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/deploy/install-a-new-windows-server-2012-active-directory-forest--level-200-

The name of the domain used for this build is AcmeFinancial.com.

2.3.4 DNS Configuration

1. Create the following host records in the AcmeFinancial.com forward lookup zone:

Name	FQDN	IP address
Activedirectory	Activedirectory.acmefinancial.com	192.168.19.10
ADBackup	ADBackup.acmefinancial.com	192.168.19.12
ConsoleWorks	Consoleworks.acmefinancial.com	192.168.17.11
Openldap	Openldap.acmefinancial.com	192.168.19.11
Racf	Racf.acmefinancial.com	172.17.212.10
RadiantOne VDS	RadiantOne VDS.acmefinancial.com	192.168.14.111
RadiantOne VDS	RadiantOne VDS.acmefinancial.com	192.168.17.100
Sharepoint2	Sharepoint2.acmefinancial.com	192.168.17.113
Splunk	Splunk.acmefinancial.com	192.168.17.10
VcenterServer	Vcenterserver.acmefinancial.com	192.168.20.6

2. Create the following IPv4 reverse lookup zones:

Name
14.168.192.in-addr.arpa
17.168.192.in-addr.arpa
19.168.192.in-addr.arpa
20.168.192.in-addr.arpa
212.17.212.in-addr.arpa

2.3.5 Installing Splunk Universal Forwarder

Note: You will need a Splunk account to download the Splunk Universal Forwarder. It is free and can be set up at: https://www.splunk.com/page/sign_up

Download the Splunk Universal Forwarder from: http://www.splunk.com/en_us/download/universal-forwarder.html

You want the latest version for OS version Windows (64-bit). Because this is installing on Windows, select the file that ends in .msi. An example is: spunkforwarder-6.4.2-00f5bb3fa822-x64-release.msi

2.3.6 Install Security Compliance Manager

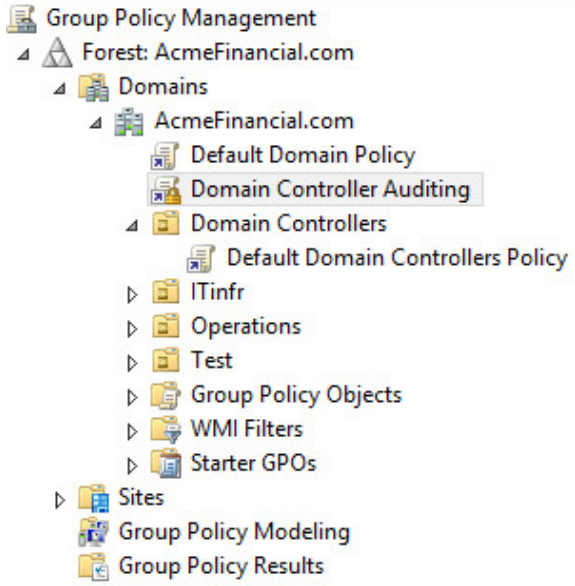
Install Microsoft Security Compliance Manager: https://www.microsoft.com/en-us/download/details.aspx?id=53353

2.3.7 Group Policy Object (GPO) Configuration

Auditing is enforced using the Microsoft Group Policy feature. Group policy auditing is administered with Microsoft Security Compliance Manager (SCM). Details for downloading and installing SCM can be found here.

SCM consist of baseline configurations based on Microsoft security guide recommendations and industry best practices. In this build, the Domain Controller Security Policy is deployed using SCM to established a benchmark. The .CAB file is included in the SCM. In our build, we deployed this benchmark named as "Domain Controller Auditing." For directions for deploying a benchmark, see the Microsoft documentation found here.

Group policy automatically applies the Default Domain Policy and Default Domain Controllers Policy when AD is installed, as shown here:

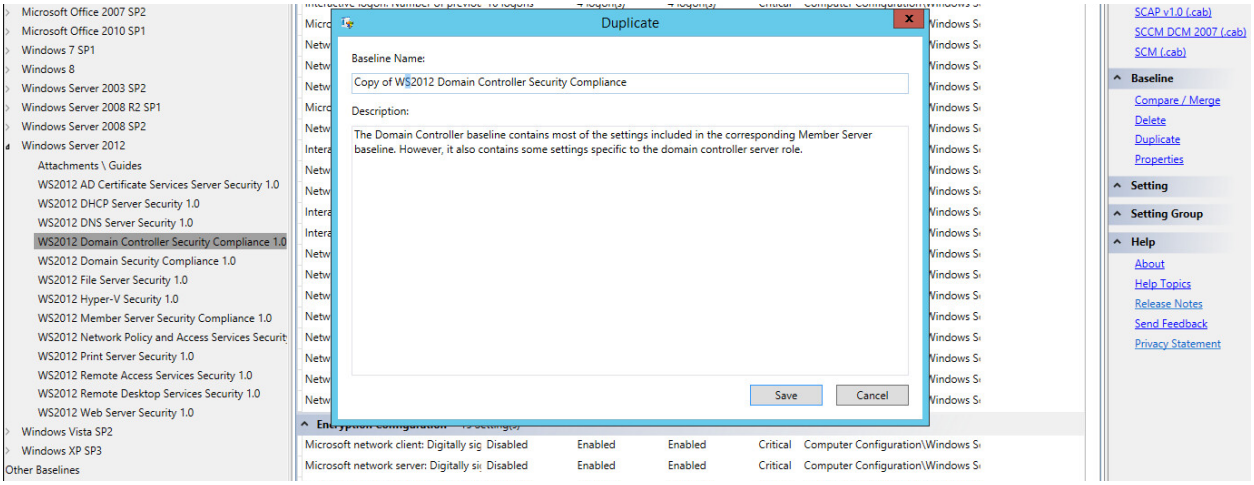


For this build, no changes are made to the Default Domain or Default Domain Controllers Policy. Both policies are *"enabled"* and *"link enabled."*

Minor changes are made to the Domain Controller Auditing Policy to enable the ability to audit user account changes, attribute changes, and policy changes for this build.

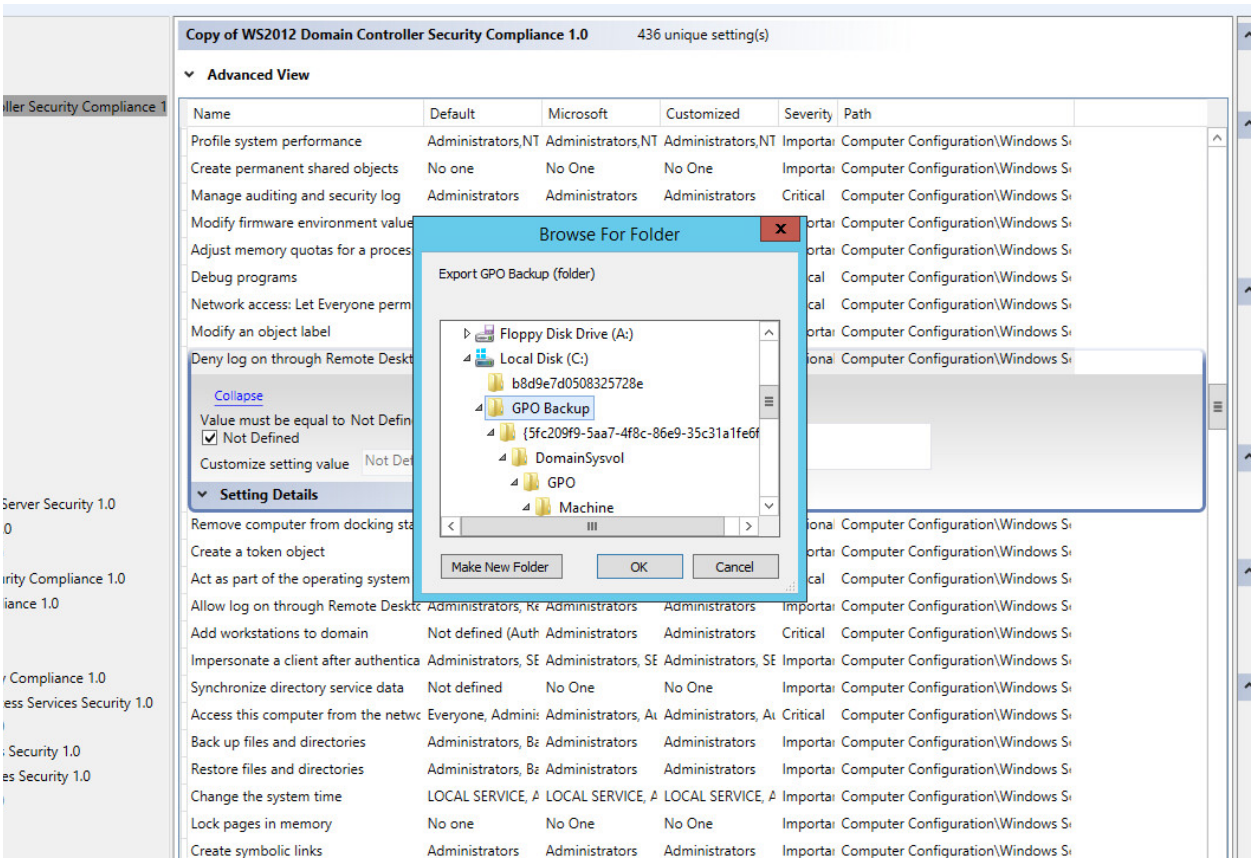
Note: This example is built in a lab environment. Some security measures were dialed back or turned off for testing purposes.

939 1. Create a duplicate of the “WS2012 Domain Controller Security Compliance 1.0” baseline. Name
940 it what you would like and save. Domain Controller Auditing is the name for this build.



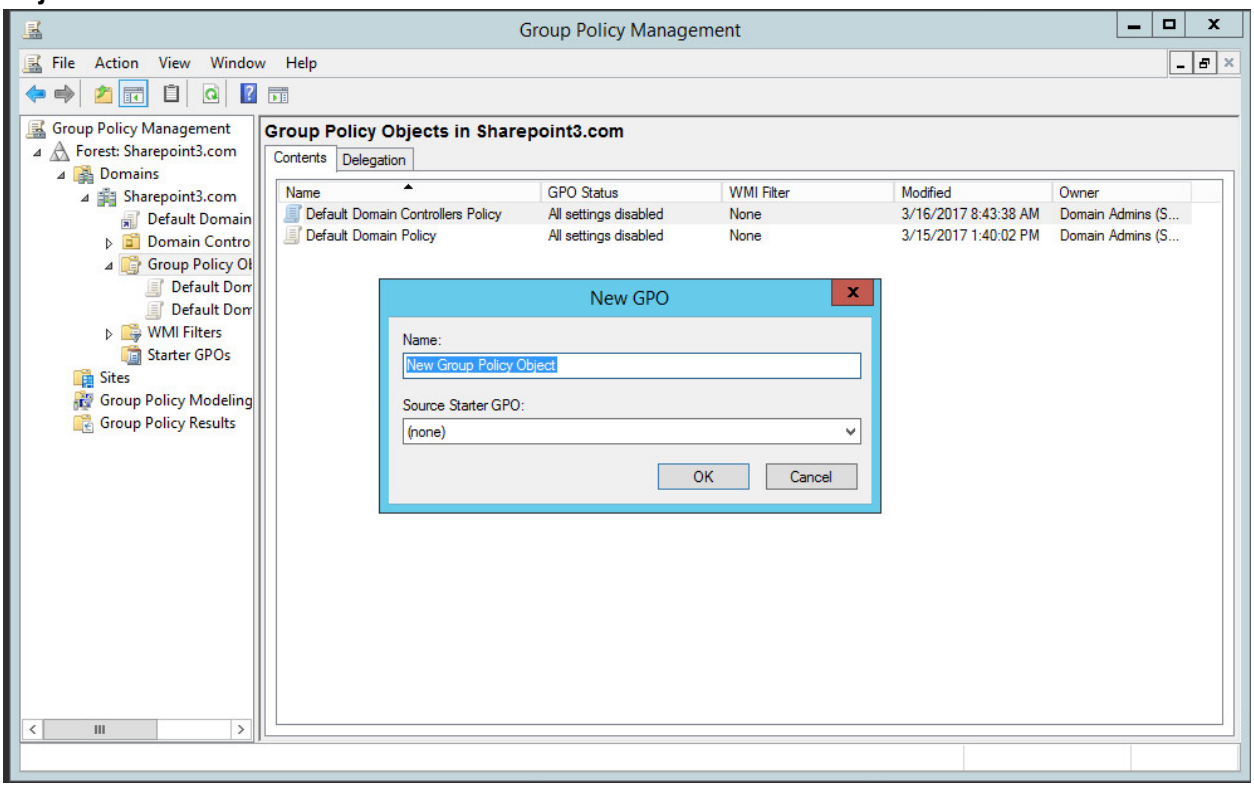
941

942 2. Export to a GPO backup folder.

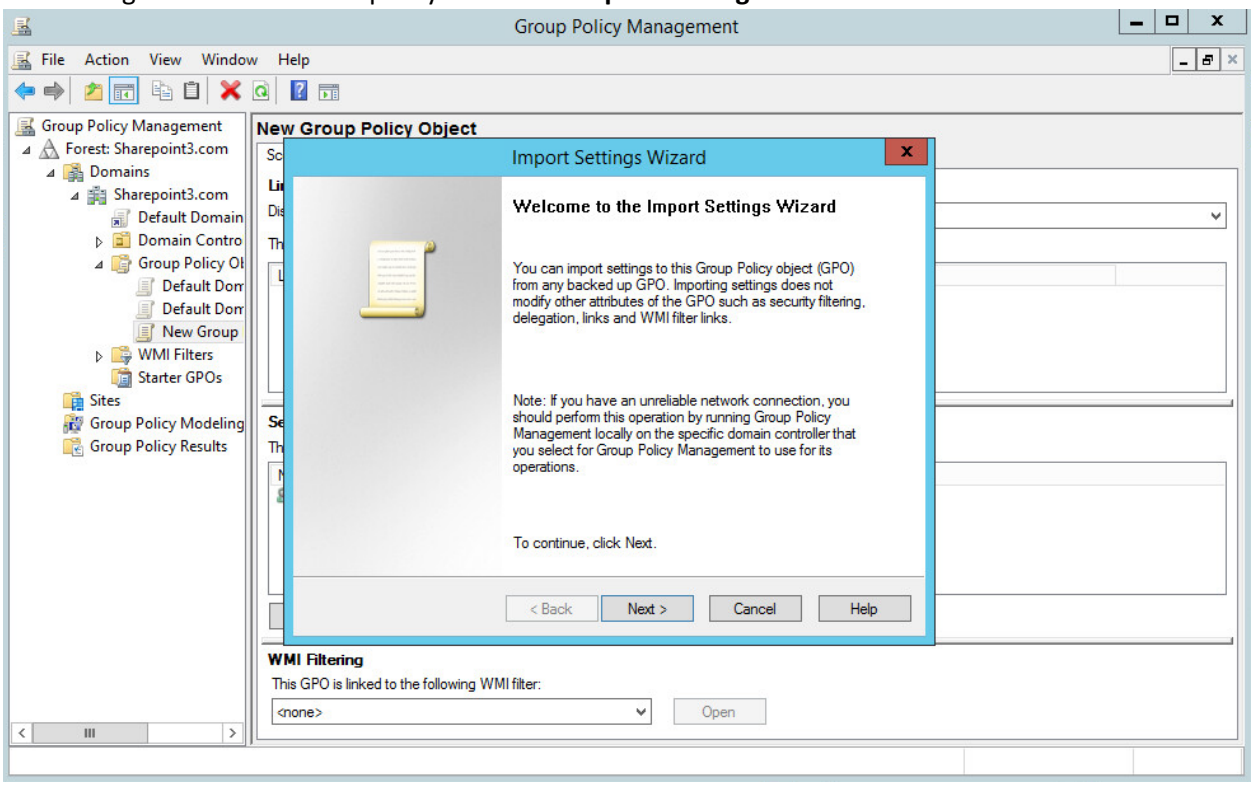


943

944 3. Open group policy management. Under the top level of the domain, right-click on **Group Policy**
945 **Object** and select **New**. Name the GPO and click **OK.**

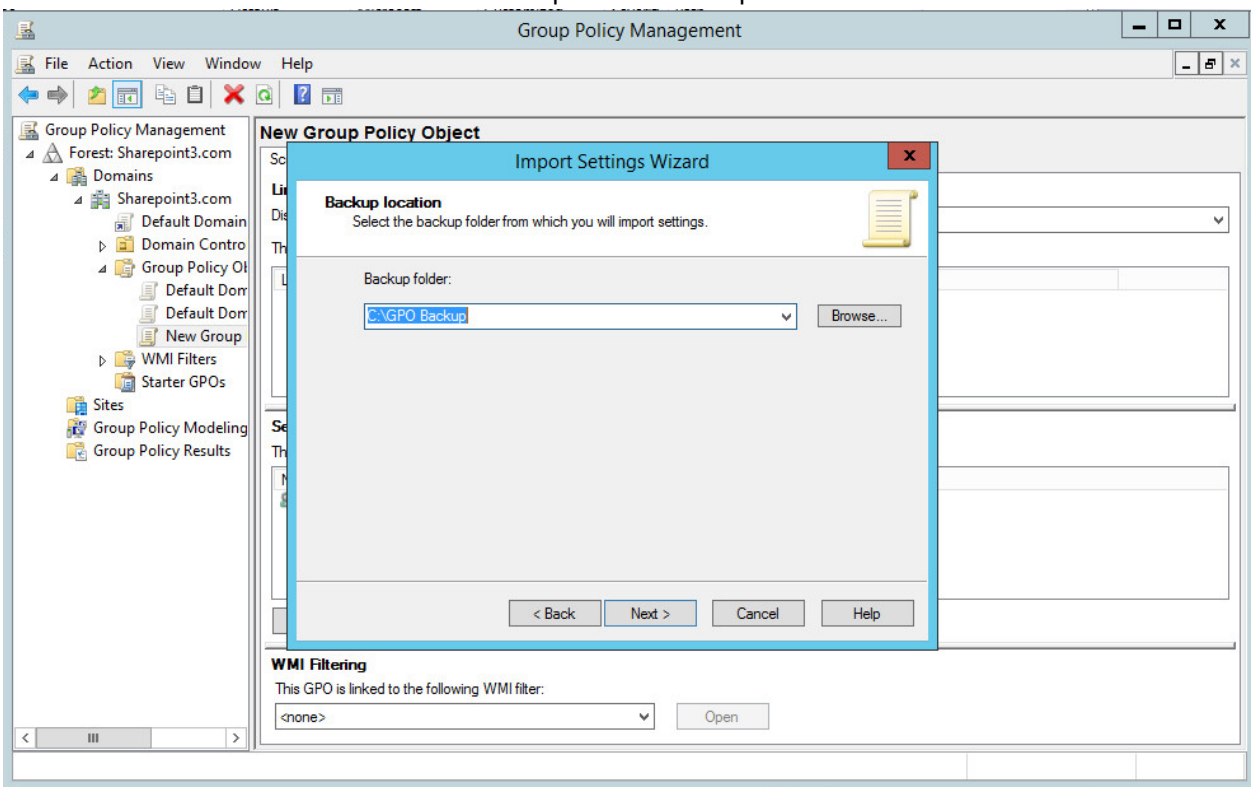


946
947 4. Right-click on the new policy and select **Import Settings**. Click **Next**.



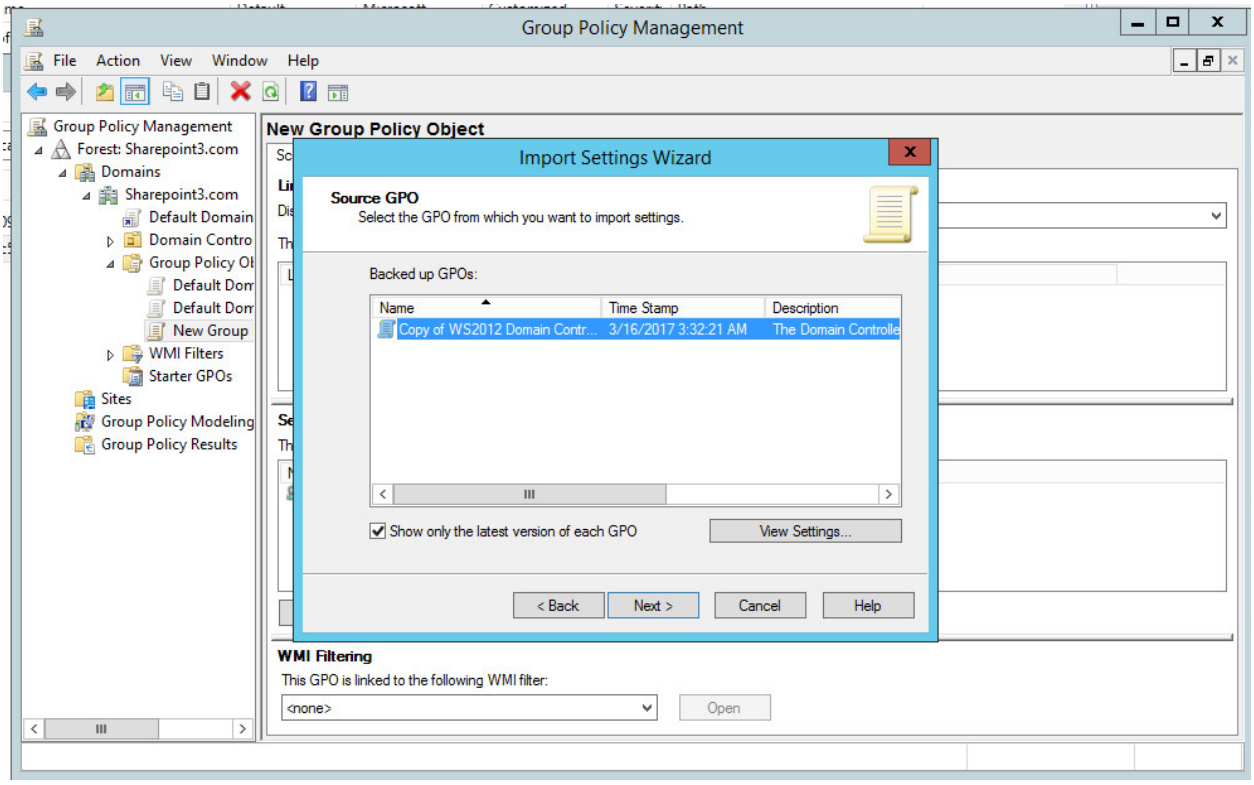
948

949 5. Select the folder location of the backup created in Step 2. Select **Next**.



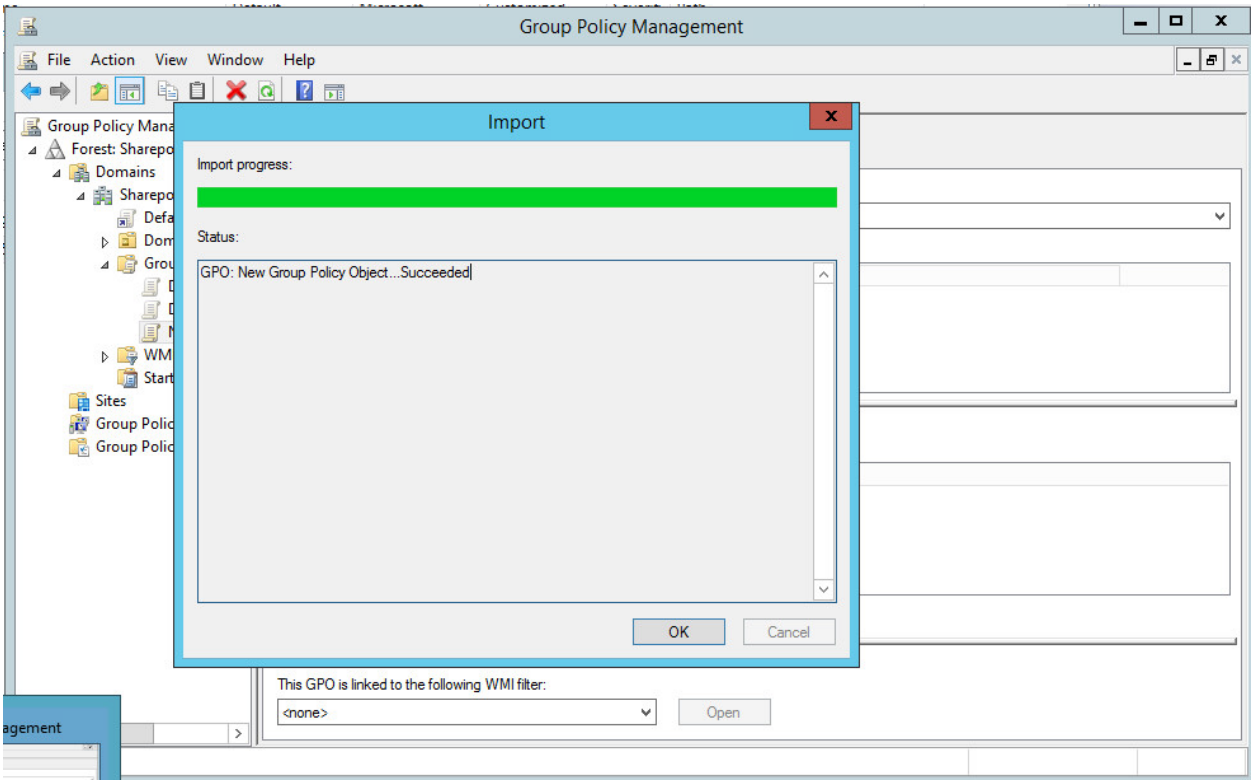
950

951 6. Select the backup created in Step 2.



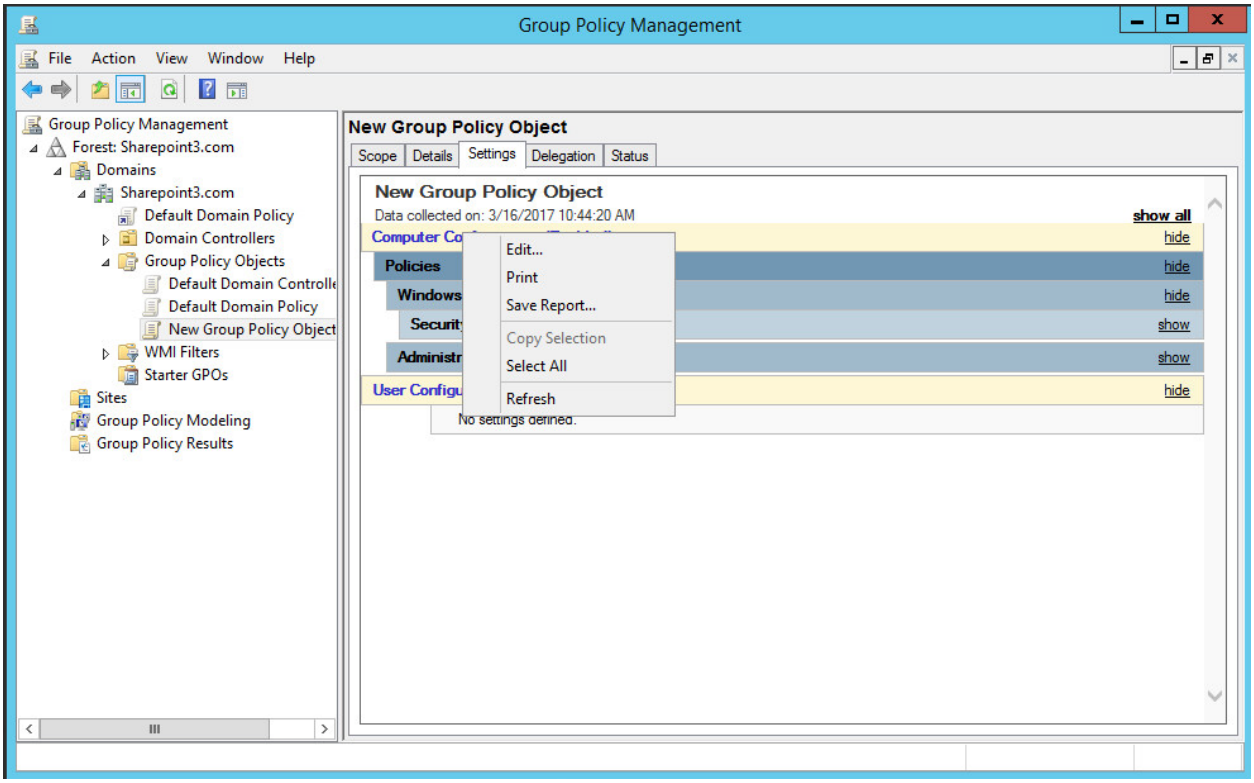
952

953 7. Click **Next** at the end of the wizard and **Finish**.



954

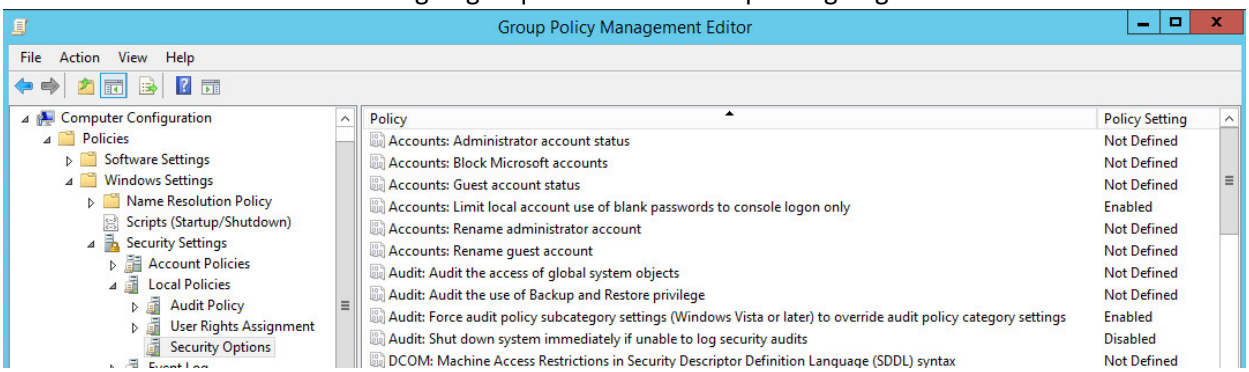
955 8. Select the new GPO, select the **Settings** tab, right-click anywhere, and select **Edit**.



956

957 9. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>Local**
958 **Policies>Security Options**. Change the value for “Audit: Force audit policy subcategory settings

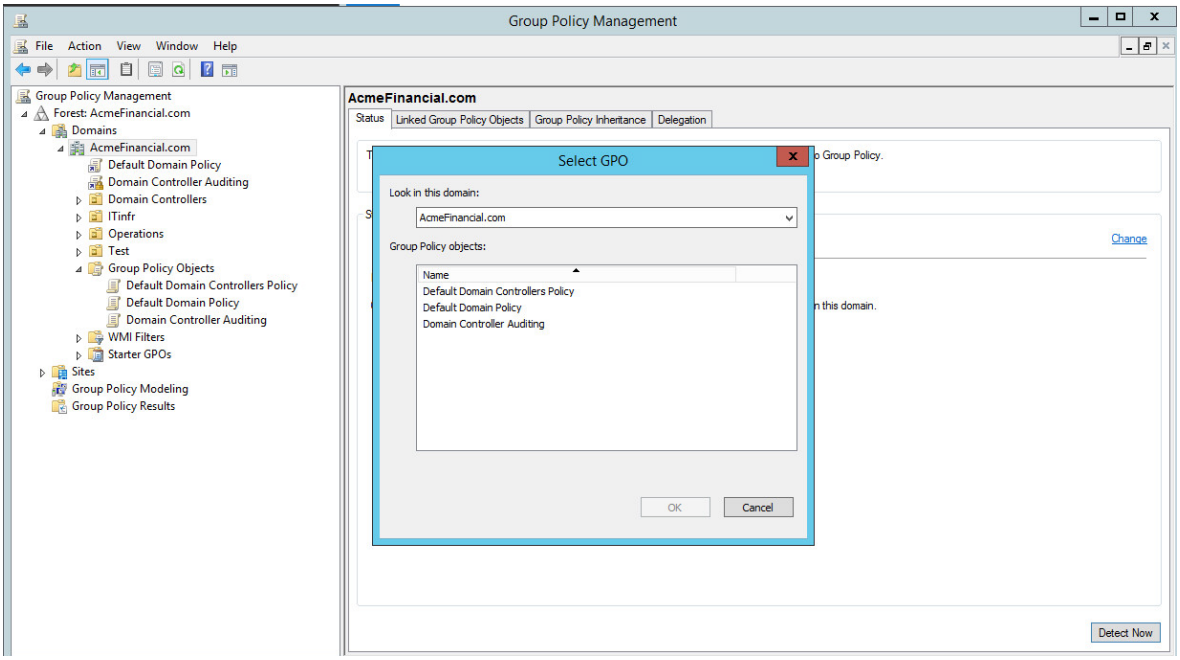
(Windows Vista or later) to override audit policy category settings" to "Enabled." Change the value for "Domain controller: LDAP server signing requirements" to "require signing."



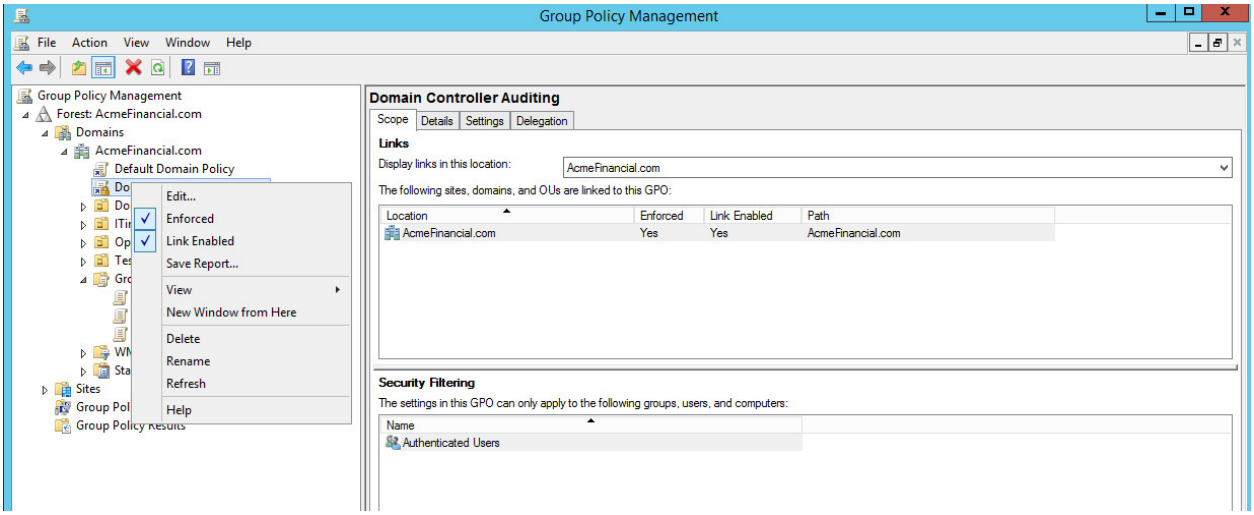
10. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>Advanced Audit Policy Configuration>Audit Policies**. Make the following changes and save:

Account Logon	
Audit Credential Validation	***Success, Failure***
Account Management	
Audit Application Group Management	***Success, Failure***
Audit Distribution Group Management	***Success, Failure***
DS Access	
Audit Directory Service Access	***No Auditing***
Audit Directory Service Changes	***Success, Failure***
Object Access	
Audit Files Share	***Success***
Audit File System	***Success***
Policy Change	
Audit Audit Policy Change	***Success, Failure***
Audit Authentication Policy Change	***Success***
Audit Authorization Policy Change	***Success***
Audit MPSSVC Rule-Level Policy Change	***Success***

964 11. Right-click on the top level of the domain again, select **Link an Existing GPO**, and choose the
965 created GPO.

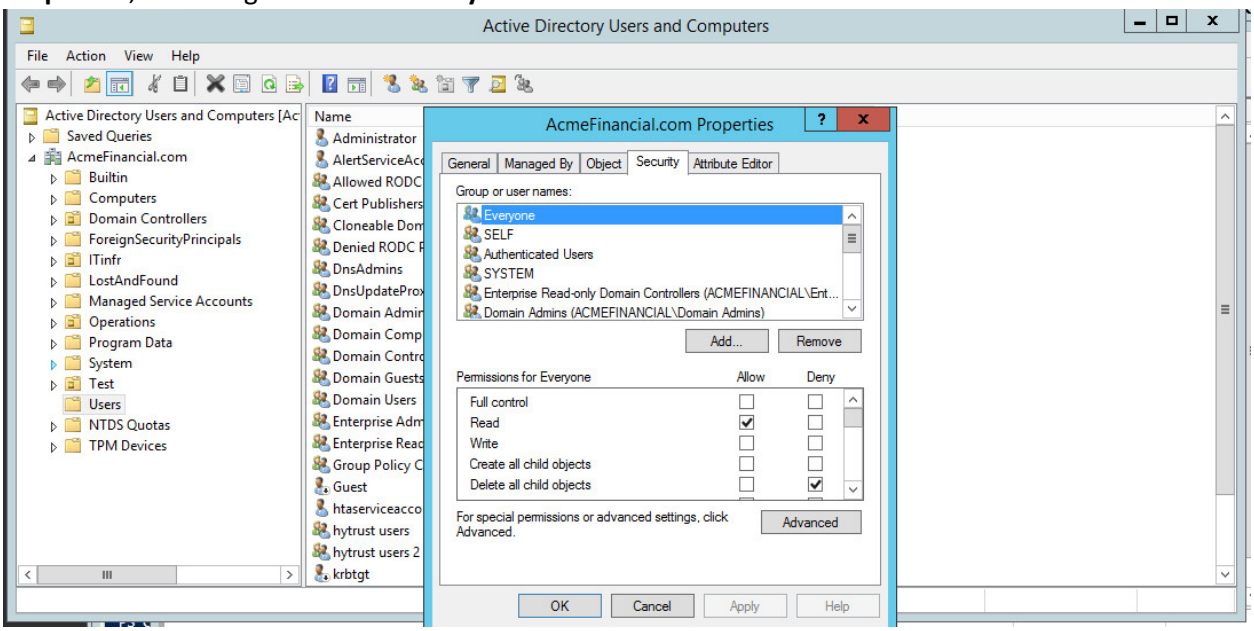


966 12. Right-click on the new GPO linked directly under the top-level domain and select **Enforced** by
967 checking it on the left.

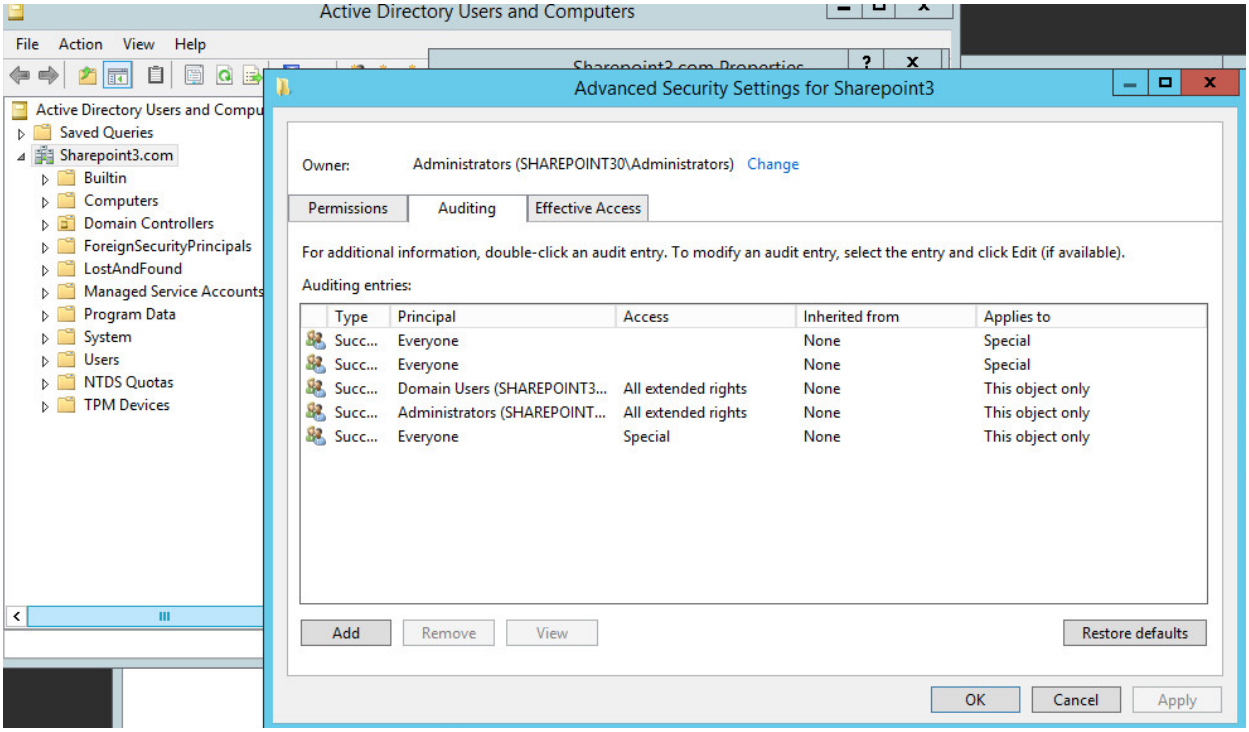


968

13. Open **Active Directory Users and Computers**, right-click on the top level of the domain, select **Properties**, and navigate to the **Security** tab.

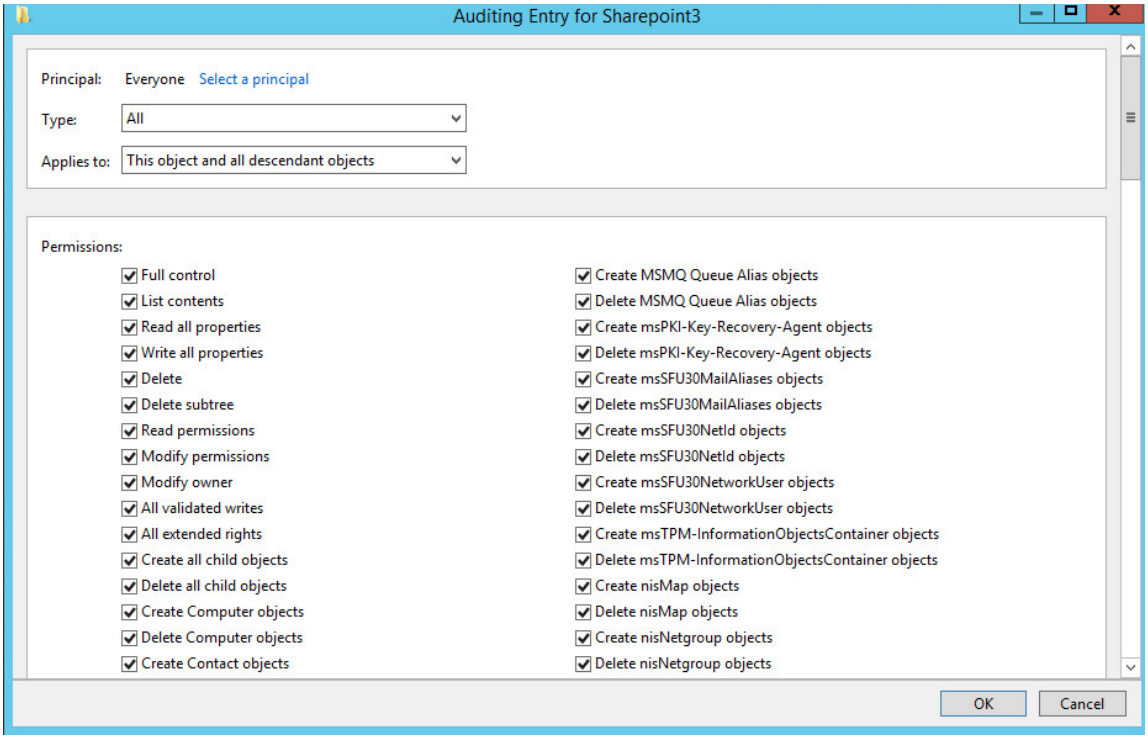


14. Select **Advanced** and navigate to the **Auditing** tab.



15. **Add** a new entry with the following parameters:

Type: *All*, Principal: *Everyone*, Applies to*: This object and all descendant objects*. Select every checkbox under "Permissions" and "Properties" to audit for each action. Click **OK** and apply the changes.



2.3.8 Script: AdDOnlineStatus.ps1

A powershell script is scheduled to run regularly on the active directory server that determines whether it is online or not and writes messages to a local file that Splunk consumes.

```
#This script determines if this server is online or offline
#If a gateway route exists, the script will
#output the current time, hostname, status and previous time (last
#time it wrote to output file)
#Check if gateway route exists
if (Get-Netroute 0.0.0.0/0)
   {
   #Store date in PrevTime variable
   $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
   #Check if prevtime-file.txt exists
   if (ls C:\scripts\prevtime-file.txt)
      {
         #Place the contents of prevtime-file.txt in the PrevTime variable
      $PrevTime=Get-Content C:\scripts\prevtime-file.txt
```

```
      }
   #Place the current date in CurrentTime
   $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
   #Overwrite the contents of prevtime-file.txt with the current date
   Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\prevtime-file.txt
   $HostVar = hostname
   $Status = 'online'
   #Add the contents of the variables CurrentTime, HostVar, Status, PrevTime to
Radiant-Status-Output.csv
   Add-Content C:\scripts\AD-Status-Output.csv
$CurrentTime','$HostVar','$Status','$PrevTime
   }
else
   {
   $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
   if (ls C:\scripts\prevtime-file.txt)
      {
      $PrevTime=Get-Content C:\scripts\prevtime-file.txt
      }
      $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
      Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\prevtime-file.txt
      $HostVar = hostname
      $Status = 'offline'
      Add-Content C:\scripts\AD-Status-Output.csv
$CurrentTime','$HostVar','$Status','$PrevTime
   }
```

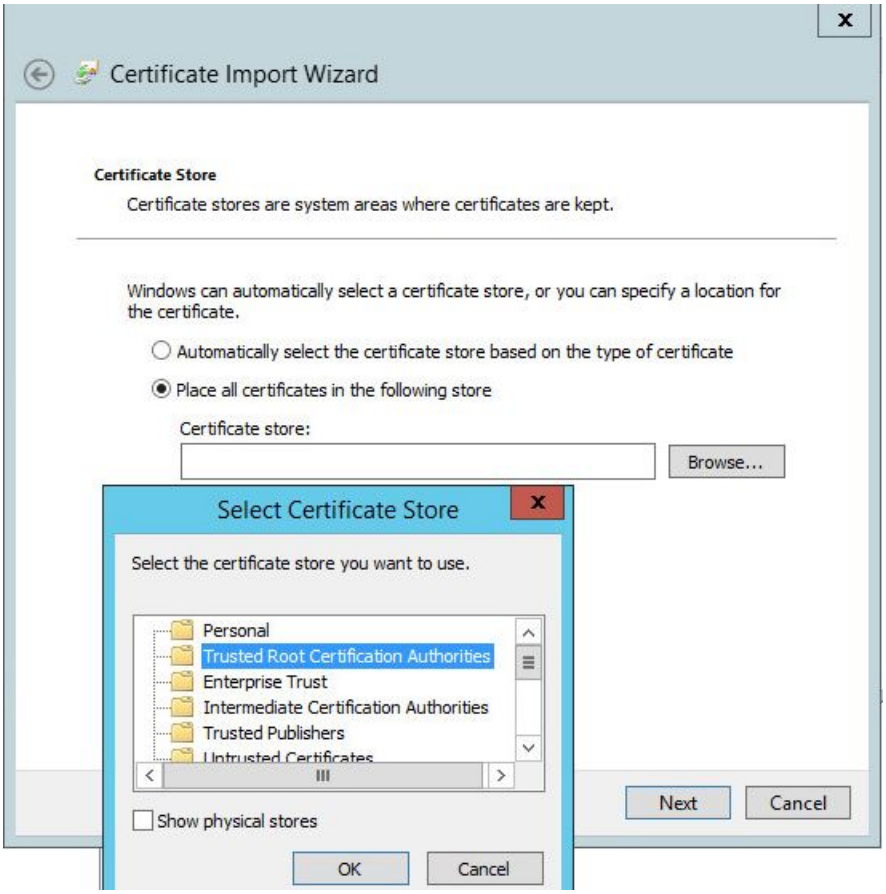
2.3.9 LDAPS Configuration

Once installed, the Active Directory service listens for both LDAP and LDAPS connections. To make LDAPS active, you will need to make sure that the certificates for the Active Directory domain controller and the certificate authority (CA) that signed the certificate are properly installed. Once these certificates are imported, LDAP clients will be able to use the LDAPS service.

1. Copy the CA and domain controller certificates over to the Active Directory domain controller.
2. Right-click on each certificate and choose **Install Certificate.**
3. Choose **Local Machine**.

4. Click **Next**
5. Choose the placement of the certificate:
    a. Choose to place the certificate in the **Personal Store** if it is the domain controller's certificate.
    b. Choose to place the certificate in the **Trusted Store** if it is the CA certificate.
6. Click **OK** and then click **Next.**

LDAPS requests can be processed at this point.



2.4 NextLabs Entitlement Manager

NextLabs Entitlement Manager is a dynamic authorization system based on Attribute Based Access Control.

2.4.1 How It's Used

NextLabs Entitlement Manager is used to authorize access to the web application, which is SharePoint in this build. Entitlement Manager requires three components for functionality: NextLabs Control Center, Policy Studio, and Entitlement Management for Microsoft SharePoint Server.

NextLabs Control Center is installed on its own server along with Policy Studio. Entitlement Management is installed on an instance of Microsoft SharePoint Server.

2.4.2 Virtual Machine Configuration

The NextLabs virtual machine is configured with:

- Windows Server 2012 R2
- 8 CPU cores
- 16GB of RAM
- 1 NIC

- 100GB of Storage

Network Configuration (Interface 1)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.14.117
Netmask: 255.255.255.0
Gateway: 192.168.14.1
DNS Name Servers: 192.168.14.1
DNS-Search Domains: n/a

2.4.3 Prerequisites

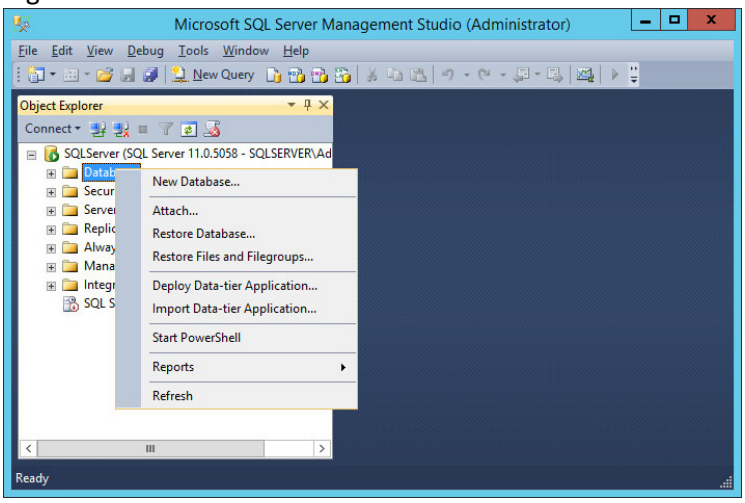
NextLabs Control Center requires an Oracle or MS SQL Server. It is recommended that the database be given 500GB of free storage space. In this build, only 100GB of storage is used for development purposes.

Additionally, multiple deployment configurations are supported. The development deployment configuration is used in this build. For this deployment, the Control Center server is deployed on the same instance as the SQL Server. For a full list of supported software and deployment configurations, see the *NextLabs Control Center Installation Guide* found at the customer portal.

2.4.4 Installing NextLabs

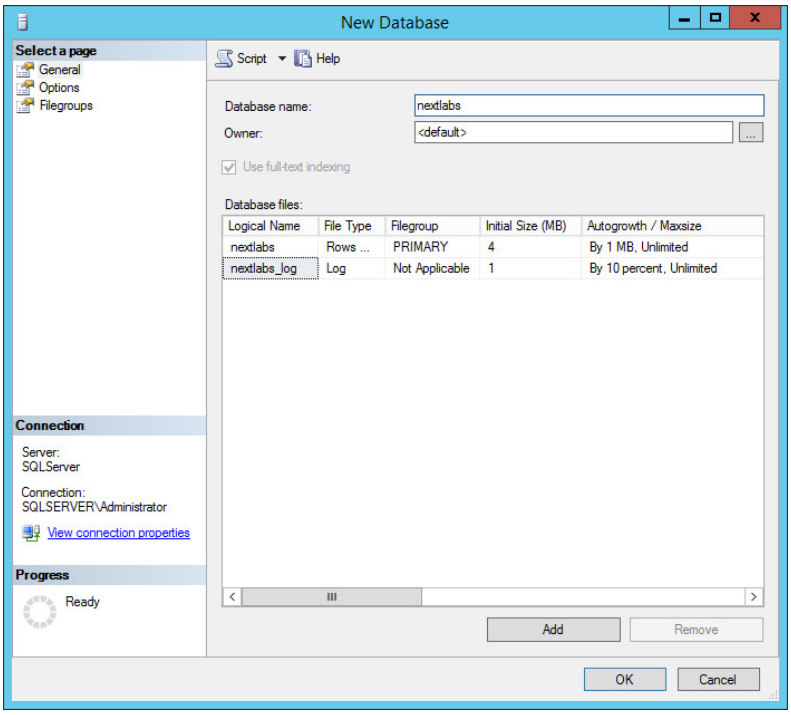
Control Center 7.7

1. Install the Microsoft SQL Server 2012 according to instructions available online.
2. Open Microsoft SQL Server Management Studio and log in to the Microsoft SQL Server.
3. Right-click on **Databases** and left-click on **New Database**.

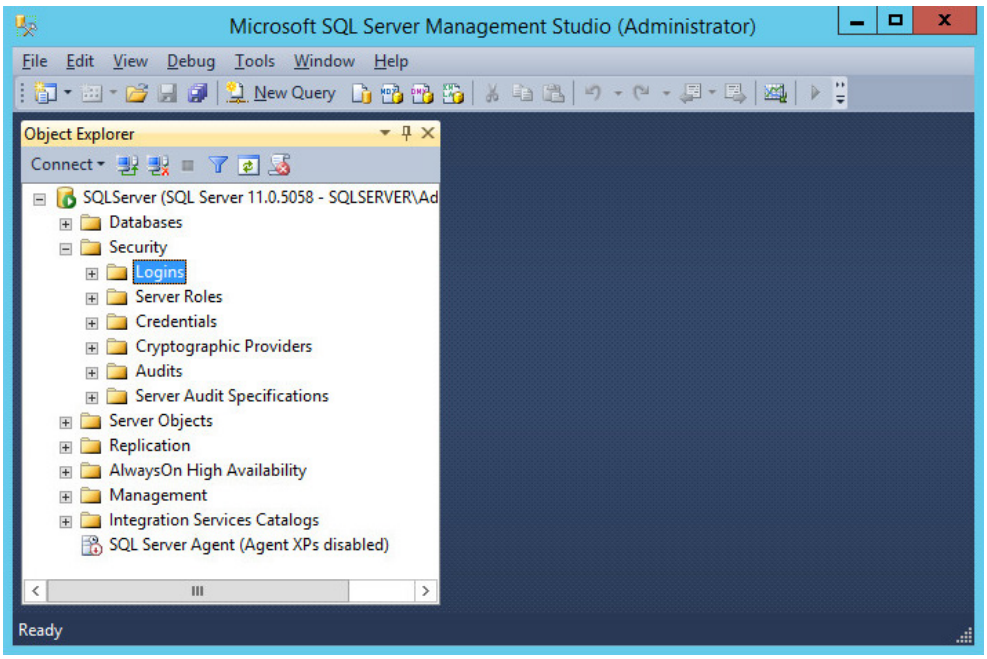


4. In the New Database window, specify a **Database name** that works for you. The application automatically copies this into the **Logical Names** of the **Database files**. Click **OK**. Example name

from this build: **nextlabs.**

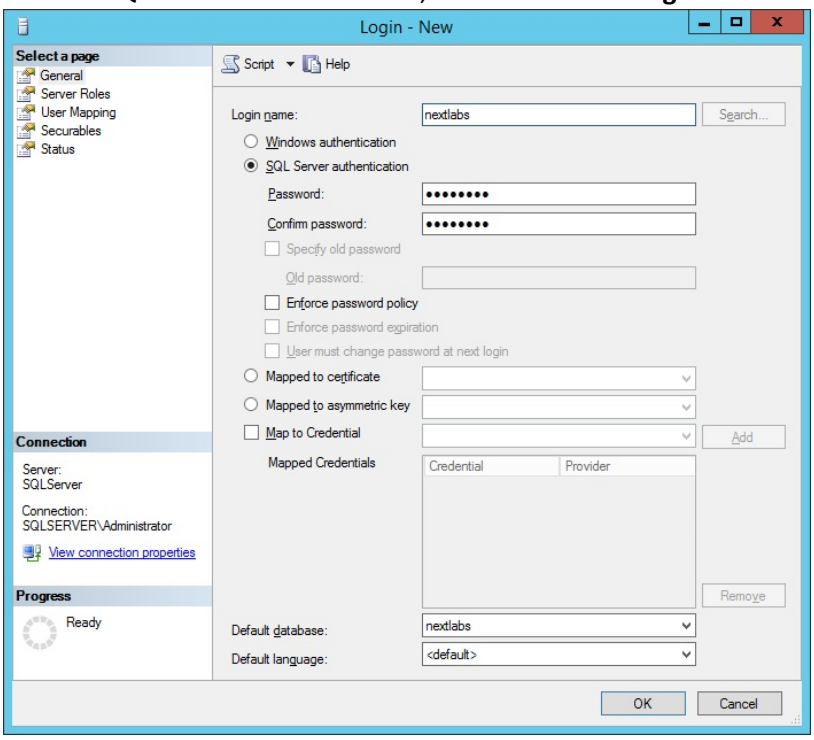


5. Click on the menu box next to **Security** to begin the process for creating a new login for the new NextLabs database's administrator.



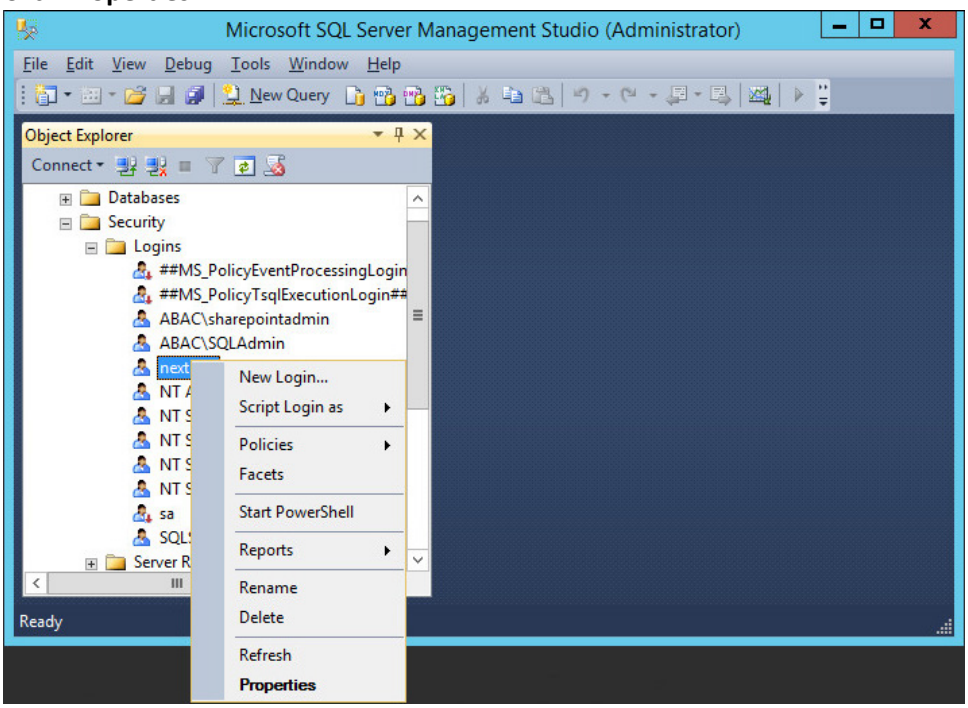
6. Right-click **Logins**. Left-click **New Login**.

1084 7. Click on **SQL Server authentication**, and enter a new **Login name** and **Password**.



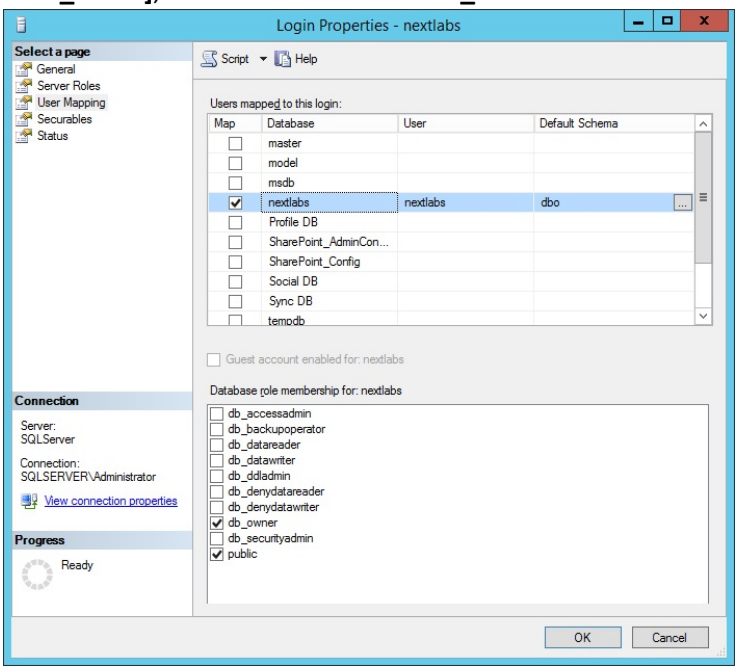
1085

1086 8. Click the menu box next to **Logins**. Right-click on the new user created in the previous step.
1087 Click **Properties**.

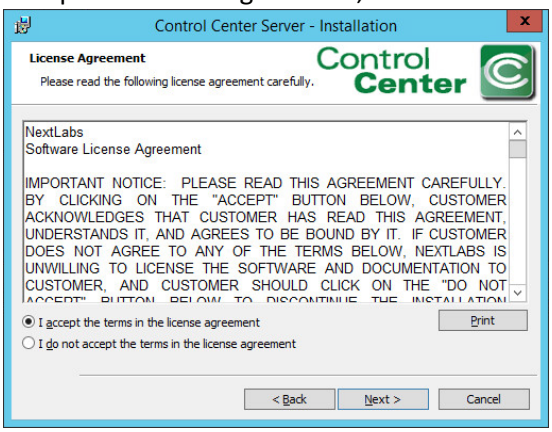


1088

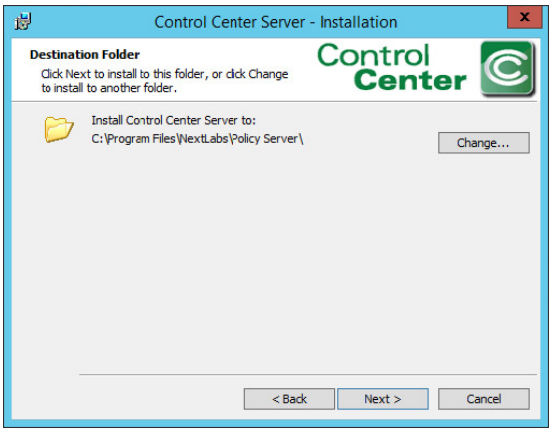
9. Click on **User Mapping**, then **New Database**. Under **Database role membership for: [database_name]**, check the box next to **db_owner**.



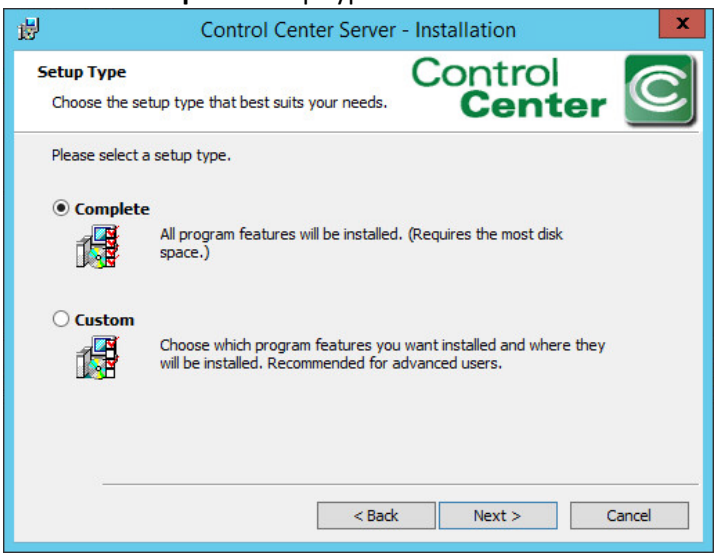
10. Locate the installation zip file, provided by NextLabs support, and extract it.
11. Run the installer as follows:
    a. On a Windows server, launch Command Prompt as Administrator.
    b. In the command prompt, navigate to the folder that contains `install.bat`. The following is an example of the cd command to type if the installation zip file is extracted in `c:\build. cd build\ControlCenter-Windows-chef-- main\PolicyServer`
12. From this directory, run the command: `install.bat`
13. Click **Next**.
14. Accept the license agreement, and click **Next.**



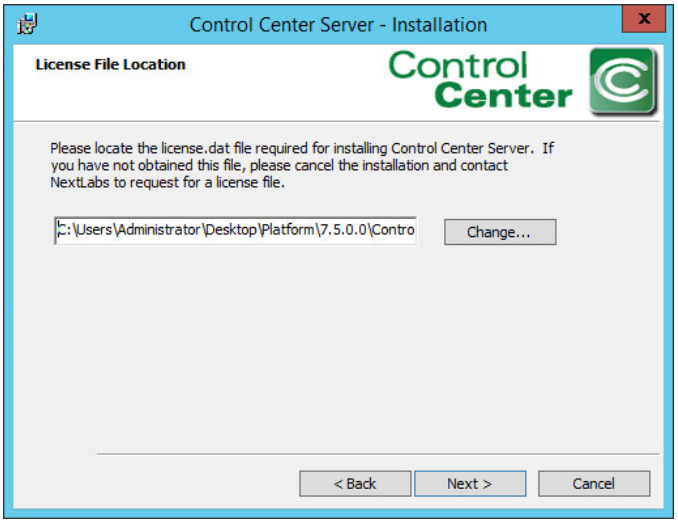
15. Click **Next.**



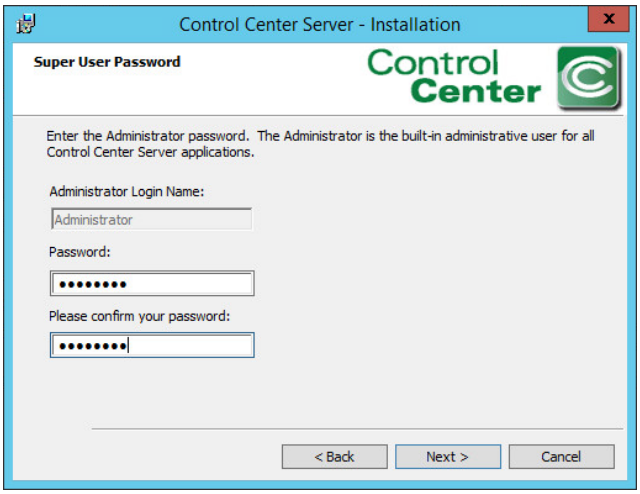
16. Select the **Complete** setup type. Click **Next.**



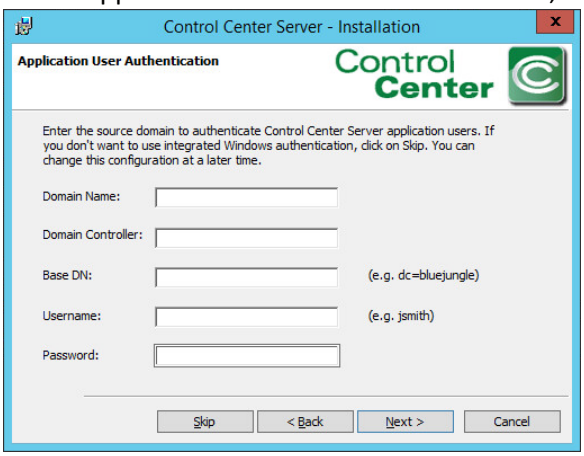
17. Enter the location of the license file. Click **Next.**



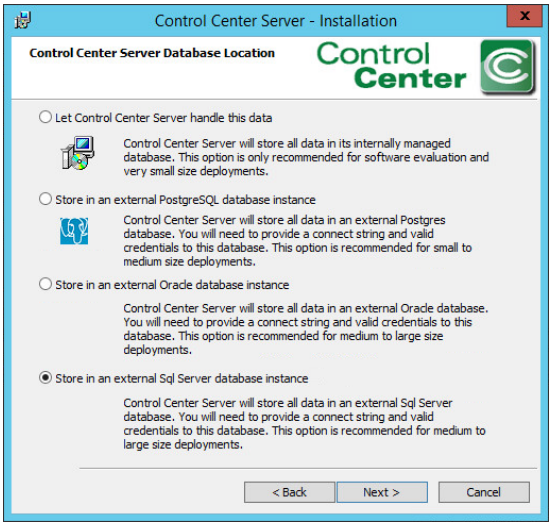
18. Enter a Password for the built-in administrative user for all Control Center Server applications. Click **Next.**



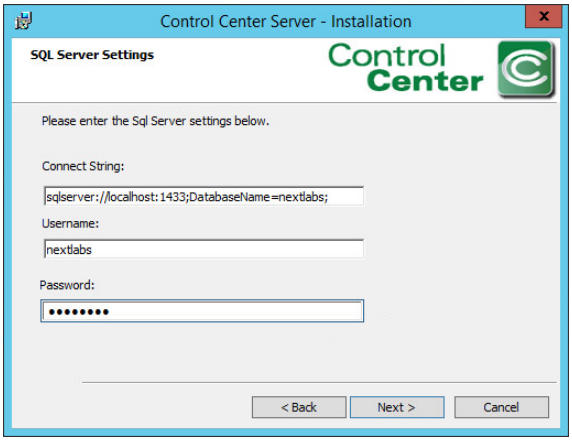
19. Enter a Password to access the SSL certificates for the Control Center Server. Click **Next.**
20. Enter a Password to access the Encryption Key Store for the Control Center Server. Click **Next.**
21. At the Application User Authentication screen, click **Skip.**



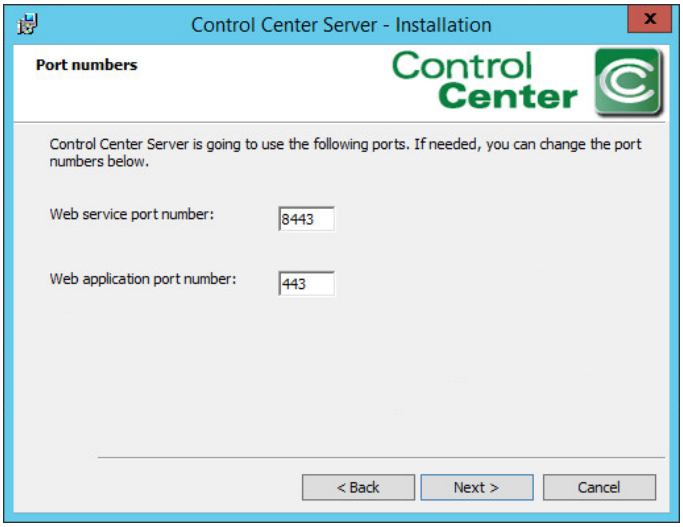
22. Select **Store in an external Sql Server database instance.** Click **Next.**



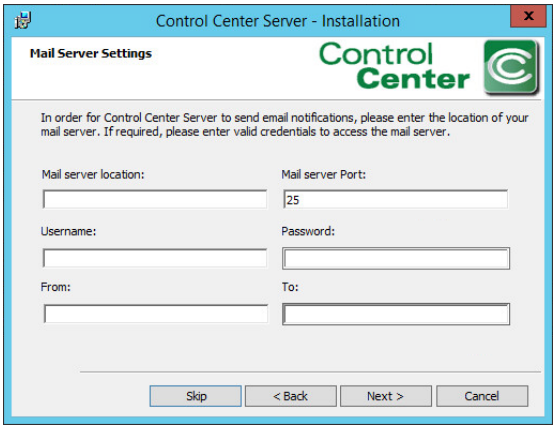
23. At the SQL Server settings screen, specify the **Connect String**, **Username**, and **Password**. Make sure the SQL Server is running. It may help to restart the SQL Server.



24. Use the default port numbers. Click **Next.**



25. Click **Skip.**



26. Click **Install.**
27. Once completed, click **Finish.**
28. Open an Internet browser, navigate to https://localhost/administrator, and log in to the Control Center Administrator web application.

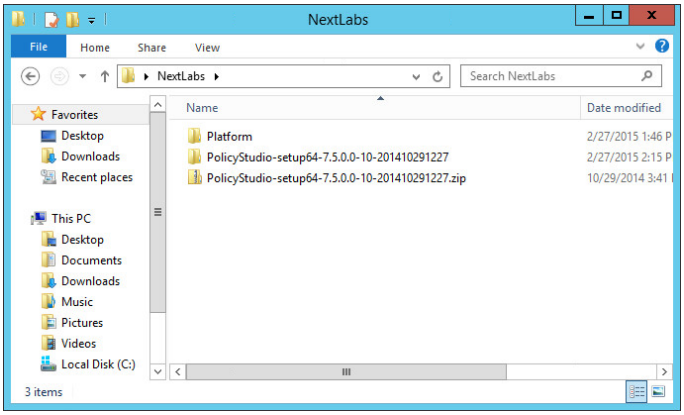
a. Enter the Administrator Username and Password to log in.

29. Once logged in to the Control Center Administrator web application in your browser, you can verify that the NextLabs Control Center is installed and configured correctly on the SQL Server.

Policy Studio 7.7

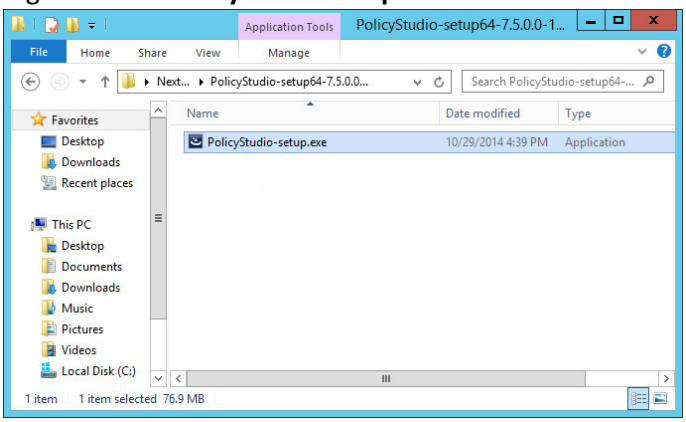
Complete the standard Policy Studio installation per NextLabs documentation available to customers using the following steps:

1. On the same server, go to your desktop or other known location where the required NextLabs Policy Studio installation files are stored.
2. Right-click on **PolicyStudio-setup64-7.5.0.0-10-201410291227.zip** and select **Extract All**. Wait for files to be extracted.

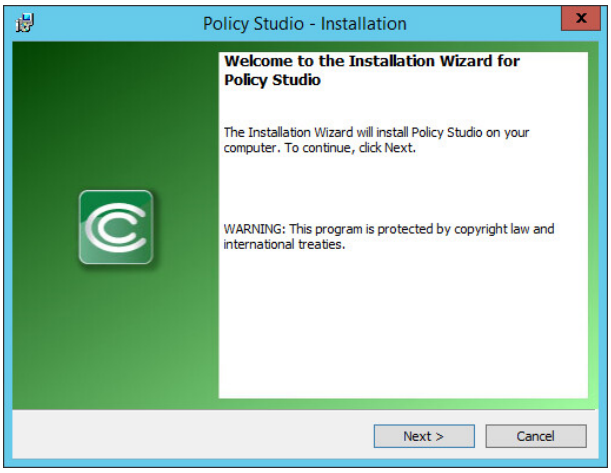


3. Double-click to open the **PolicyStudio-setup64-7.5.0.0-10-201410291227** folder.

4. Right-click on **PolicyStudio-setup.exe** and select **Run as Administrator**.

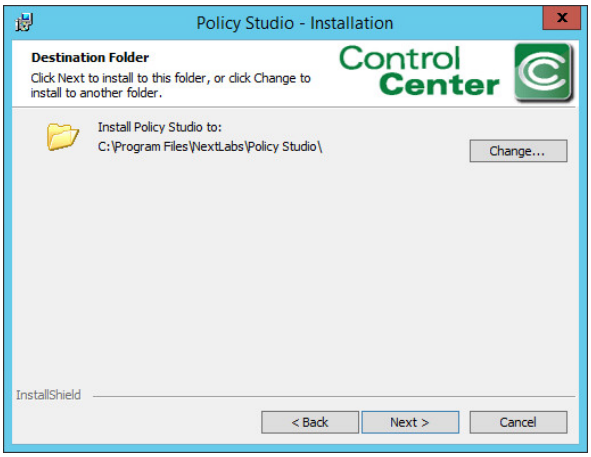


5. At the Welcome to the Installation Wizard for Policy Studio screen of the Policy Studio Installation Window, click **Next**.

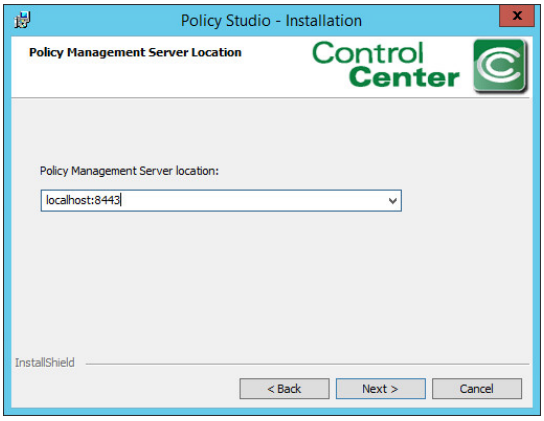


6. At the License Agreement screen, select **I accept the terms in the license agreement**, and click **Next**.

7. At the Destination Folder screen, click **Next.**

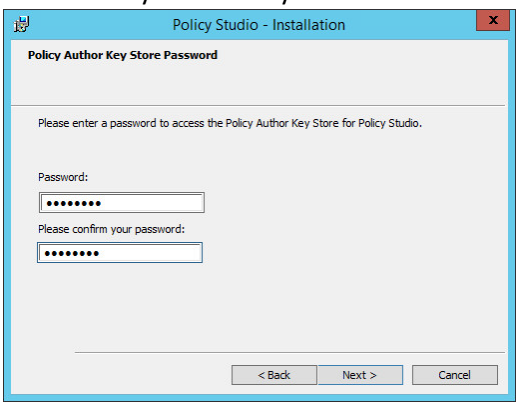


8. At the Policy Management Server Location screen, enter the default location **localhost:8443**.

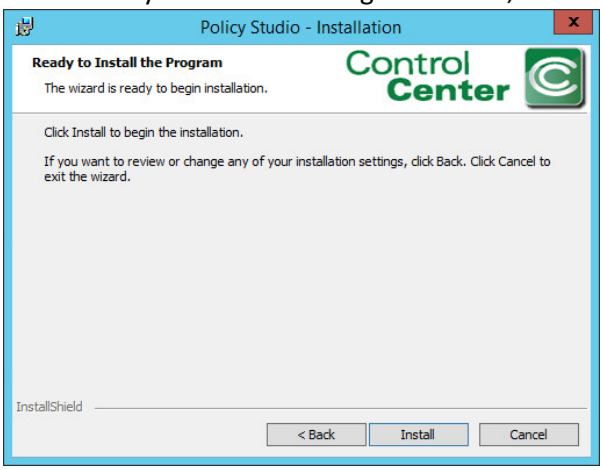


Click **Next**.

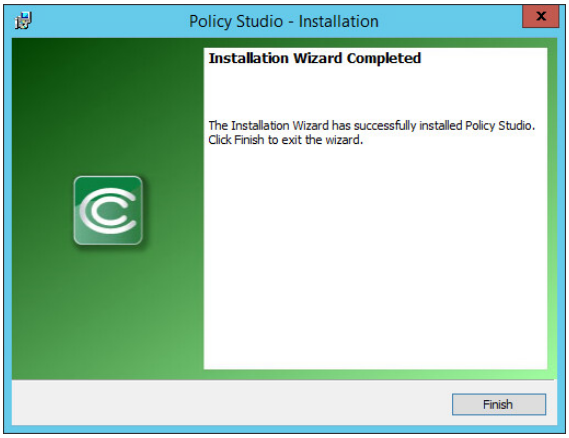
9. At the Policy Author Key Store Password screen, enter a **Password** and click **Next**.



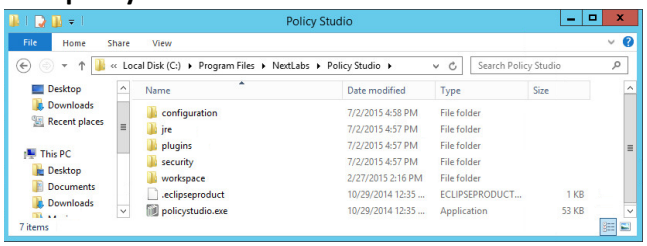
10. At the Ready to Install the Program screen, click **Install**.



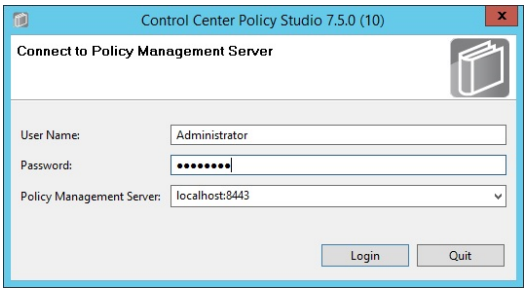
11. At the Installation Wizard Completed screen, click **Finish**.



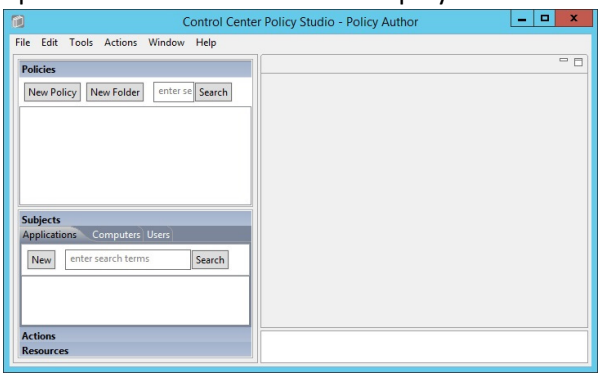
12. In Windows Explorer, find and open the **policystudio.exe** application file.
    a. Navigate to the **C:/ drive>Program Files>NextLabs>Policy Studio**.
    b. Click **policystudio.exe**.



13. In the Control Center Policy Studio window, enter a **User Name** and **Password** to connect to the Policy Management Server.



14. If the connection is successful, the Control Center Policy Studio - Policy Author window will open. Policies are defined and deployed in this interface.

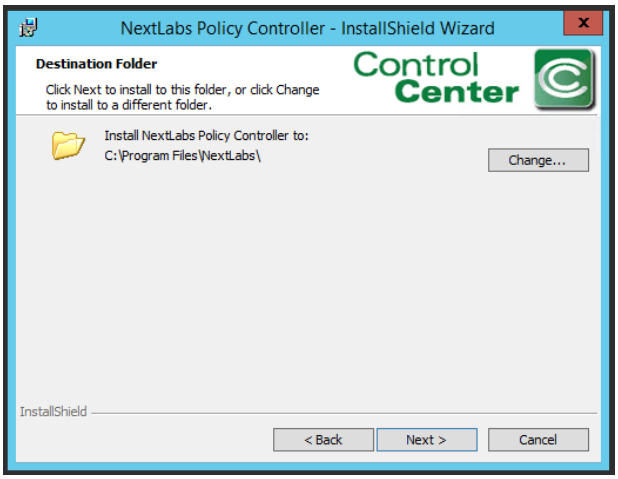


Policy Controller 7.7

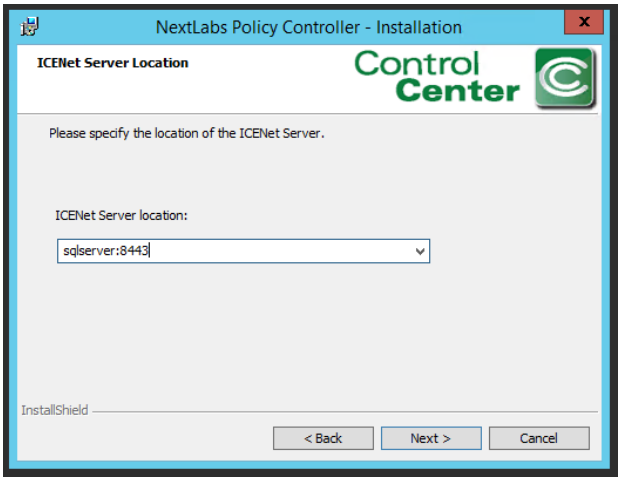
The Policy Controller is installed on the SharePoint Server. To complete standard Policy Controller installation per NextLabs documentation available to customers, use the following steps:

1. On the SharePoint Server, go to your desktop or other known location where the required NextLabs Policy Controller installation files are stored.
2. Extract the files from the **PolicyController-CE-64-<version>.zip** file.
3. Open the **PolicyController-CE-64-<version>** folder.
4. Click **CE-PolicyController-setup64.msi** to begin installation.
5. At the Welcome to the InstallShield Wizard for NextLabs Policy Controller Installation screen, click **Next**.
6. At the License Agreement screen, select **I accept the terms in the license agreement** and click **Next**.

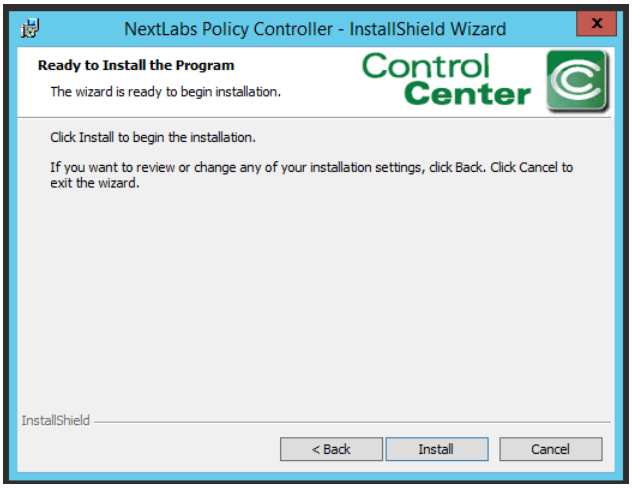
7. At the Destination Folder screen, click **Next**.



8. At the ICENet Server Location screen, enter the default ICENet Server Location: sqlserver:8443. Click **Next**.



9. At the Ready to Install the Program screen, click **Install**.



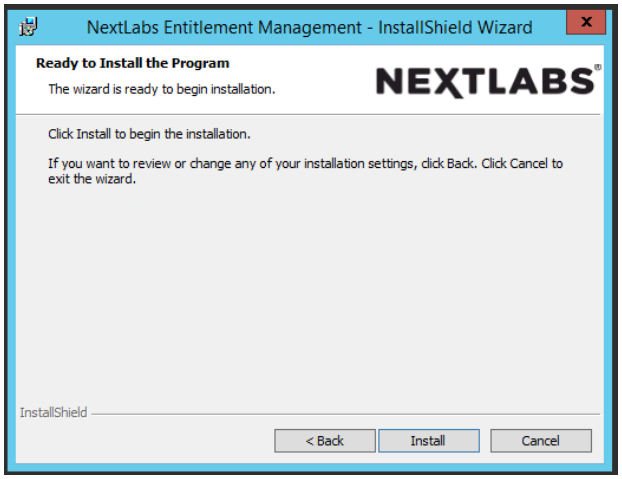
10. At the InstallShield Wizard Completed screen, click **Finish**.

11. In the window that immediately opens, click **Yes** to restart the computer, or click **No** to wait and restart after installing Entitlement Manager.

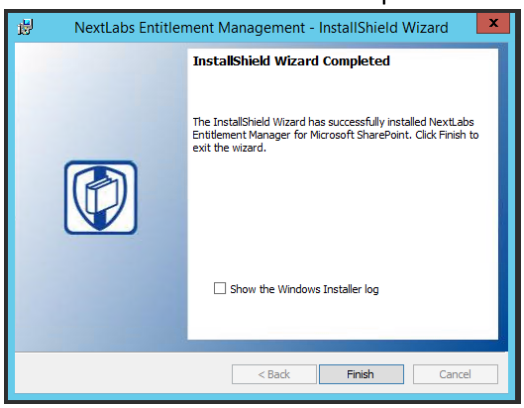
Entitlement Manager for Microsoft SharePoint 7.6

Entitlement Manager is installed once SharePoint and the Policy Controller have been installed. The web application site and site collection must already exist in SharePoint. See Section 2.7 for installing SharePoint and creating site collections. Complete the standard Entitlement Manager for SharePoint Server installation per NextLabs documentation available to customers using the following steps.

1. On the SharePoint Server, go to your desktop or other known location where the required NextLabs Policy Controller installation files are stored.
2. Extract the files from the **SharePointEnforcer-2013-64-<version>.zip** folder.
3. Open the **SharePointEnforcer-2013-64-<version>** folder.
4. Click on the **SharePointEnforcer-2013-64-<version>.msi** to begin the installation.
5. At the Welcome to the InstallShield Wizard for NextLabs Entitlement Manager for MicroSoft Share-Point screen, click **Next**.
6. At the License Agreement screen, select **I accept the terms in the license agreement** and click **Next**.
7. At the Ready to Install the Program screen, click **Install**.



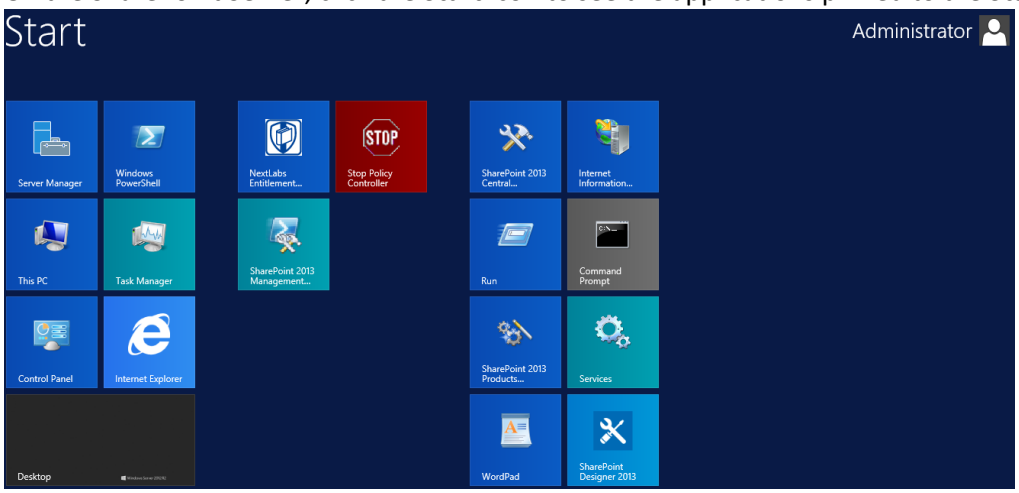
8. At the InstallShield Wizard Completed screen, click **Finish**.



9. After installing, the IIS server must be reset:
    a. Click the Windows icon and begin typing the word **PowerShell** and open the windows PowerShell application.

b. From within the Windows PowerShell window, type in this command and press **Enter** to reset Internet Information Services: **iisreset.**

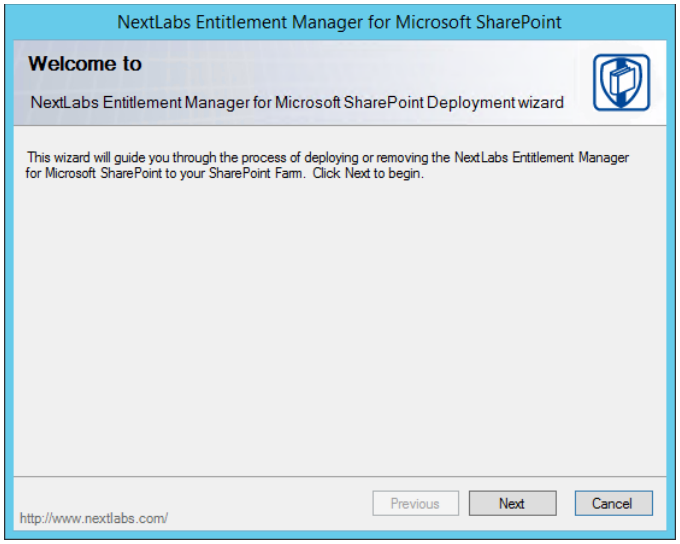
10. On the SharePoint Server, click the **Start** icon to see the applications pinned to the **Start** menu.



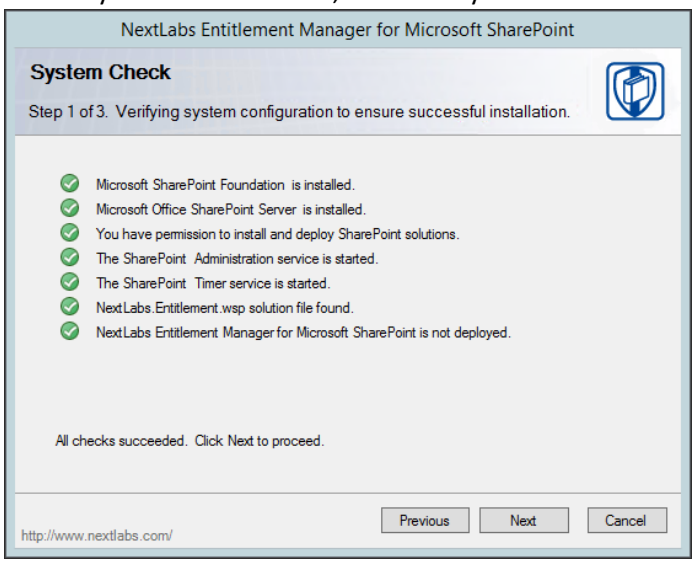
11. Click the NextLabs Entitlement Manager for SharePoint Server Deployment icon.

This shortcut is automatically pinned during the initial installation. In case the shortcut is not created automatically, the application can be opened from File Explorer at the **location: C:\Program Files\NextLabs\SharePoint Enforcer\bin\NextLabs.Entitlement.Wizard.exe**

12. At the Welcome to NextLabs Entitlement Manager for Microsoft SharePoint Deployment wizard screen, click **Next**.



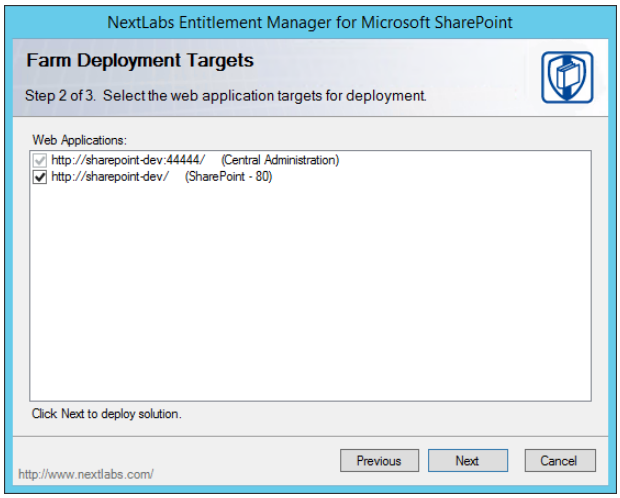
13. At the System Check screen, after the system check is complete, click **Next**.



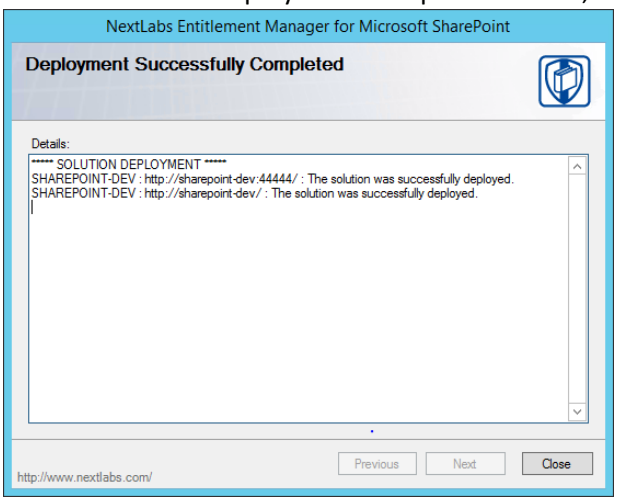
14. At the Farm Deployment Targets screen, select the applicable web application on which to deploy.

    Note: If only one entry is listed, i.e., **http://sharepoint:44444/Central Administration**, no web applications have been created.

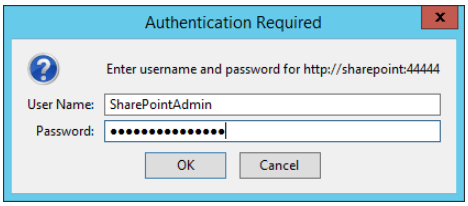
15. At the Deploying Step 3 of 3 screen, click Next.



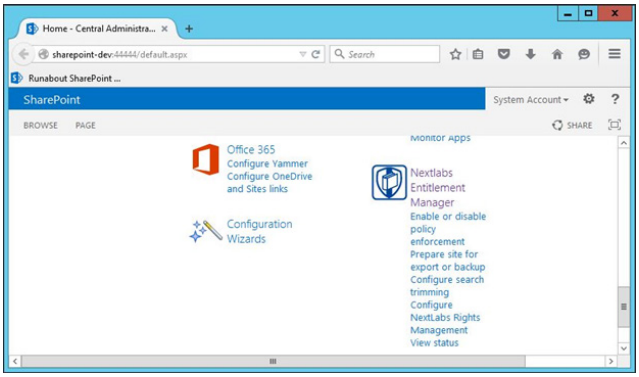
16. At the Successful Deployment Completed screen, click **Close**.



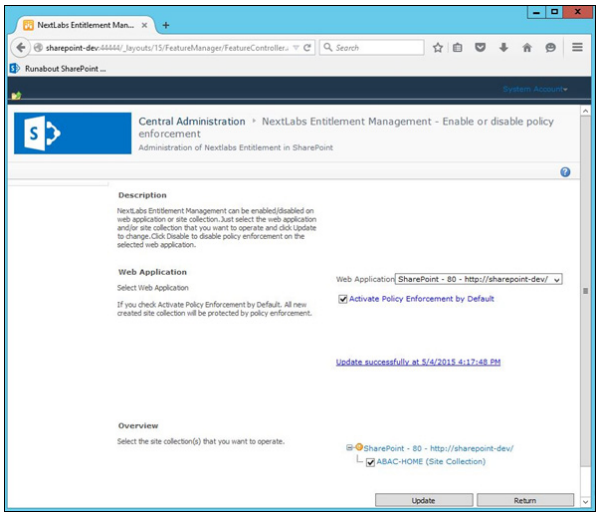
17. Open a browser and navigate to the SharePoint Central Administration Portal. Log in with the SharePoint Administrator account.



18. Click on the **NextLabs Entitlement Manager** icon.



19. In the page that opens, scroll down to verify that the correct **Web Application** is chosen and the service is **Enabled**.



2.5 OpenLDAP

OpenLDAP is an open source implementation of the Lightweight Directory Access Protocol. It stores user identity information along with various other attributes that are indicative of access rights, and it is able to provide the necessary information that requesting services need to make authorization decisions.

2.5.1 How It's Used

OpenLDAP stores user information and associated attributes for users who need access to Unix/Linux based applications. Examples of such attributes are a user's userid, group, organizational unit, job title and various other custom attributes. The OpenLDAP service listens and responds to requests from the virtual directory service that acts as the enterprise policy information point and has the responsibility for retrieving, organizing, and aggregating each user's attribute set under a single view.

2.5.2 Virtual Machine Configuration

The OpenLDAP virtual machine is configured aas follows:

- Ubuntu Linux 16.04 LTS
- 1 CPU core
- 2GB of RAM
- 2 NICs
- 60GB of storage
- OpenLDAP server software

Network Configuration (Interface 1)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.19.11
Netmask: 255.255.255.0
Gateway: 192.168.19.1

DNS Name Servers 192.168.19.10
DNS-Search Domains: acmefinancial.com

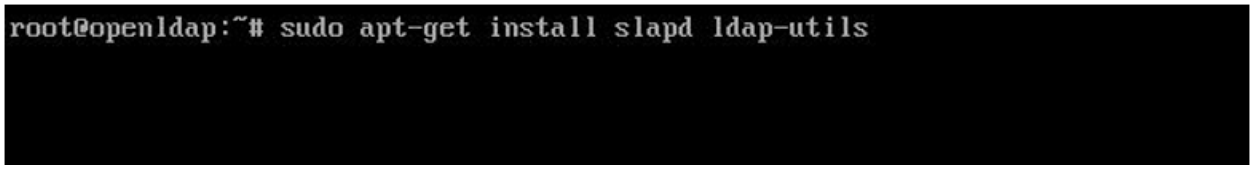
Network Configuration (Interface 2)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.19.11
Netmask: 255.255.255.0
Gateway: 192.168.19.1
DNS Name Servers 192.168.19.10
DNS-Search Domains: acmefinancial.com

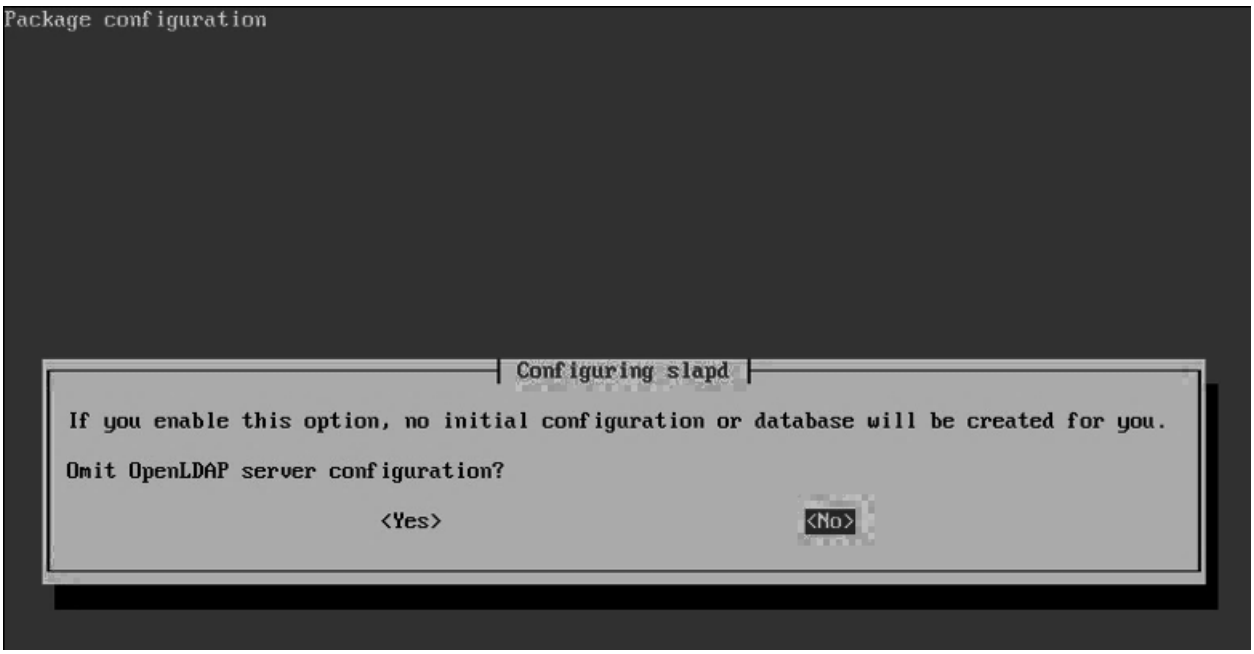
2.5.3 Firewall Configuration

Enter the following commands in sequence to allow traffic to LDAPS and SSH ports only.

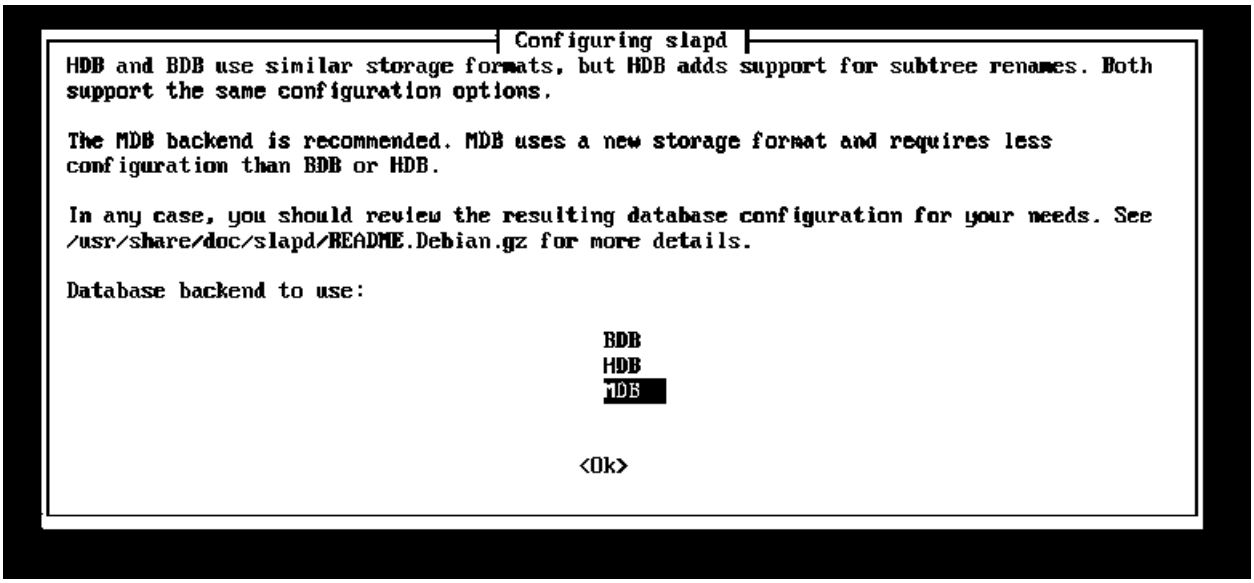
```
ufw allow 636/tcp to allow
ufw allow 22/tcp to allow
ufw default deny incoming
```

2.5.4 Installation





1. Select **No** and press **Enter.**
2. Enter the organizational Name on the following screen (for example, acmefinancial.com).
3. Enter the administrator password for the BaseDN (BaseDN: acmefinancial.com).

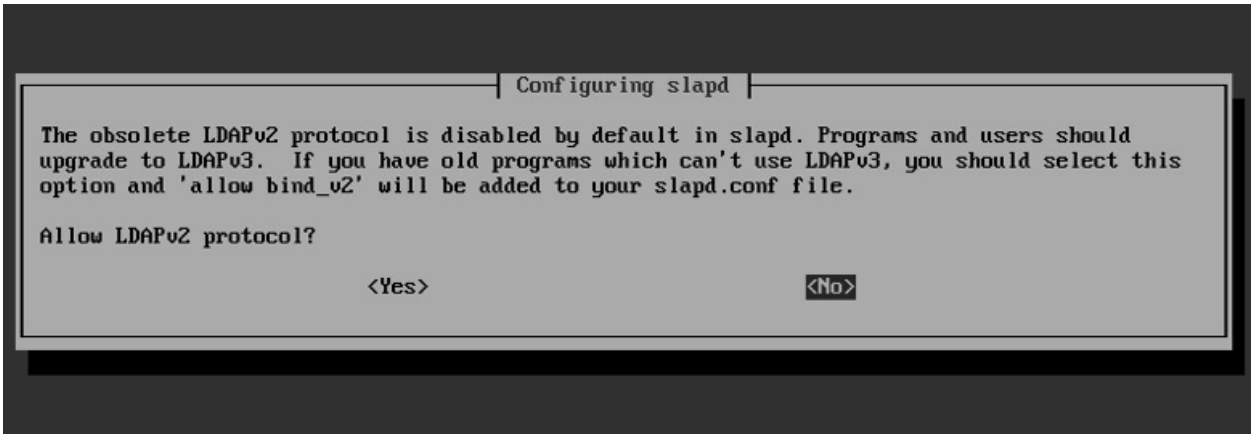


1285

1286 4. Select **MDB** as the Backend database for OpenLDAP and press **Enter**.

1287

1288 5. Select **No** and press **Enter**.



1289

1290 6. **Select No** to disable LDAPv2.

1291 2.5.5 Audit Configuration

1292 1. Enter `mkdir /etc/ldap/logs` at a shell prompt to create a directory that is writable by the
1293 OpenLDAP service.

2. Enter `chown openldap.openldap /etc/ldap/logs` to make the logs subdirectory owned by the openldap service.
3. Enter `touch create-cn-module.ldif` to create a file that will be used to load a cn module. This will allow the AuditLogConfig object class to be added. The file contents should be as follows:

```
dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/lib/ldap
olcModuleLoad: auditlog.la
```

4. Enter `ldapadd -Q -Y -EXTERNAL -H ldapi:/// -f create-cn-module.ldif` to add the cn module.
5. Enter `touch logging.ldif`. The file contents should be as follows:

```
dn: olcOverlay=auditlog,olcDatabase={1}hdb,cn=config
changetype: add
objectClass: olcOverlayConfig
objectClass: olcAuditLogConfig
olcOverlay: auditlog
olcAuditlogFile:/etc/ldap/logs/auditlog.log
```

6. Enter `chmod 775 /etc/ldap/logs`.
7. Enter `chmod 664 /etc/ldap/logs/auditlog.log`.
8. Enter `ldapadd -Q -Y -EXTERNAL -H ldapi:/// -f logging.ldif`.
9. Changes to user records should now appear in /etc/ldap/logs/auditlog.log.

2.5.6 STARTTLS and LDAPS Configuration

1. On the OpenLDAP server, create an ssl directory /etc/ldap/ssl. Enter `mkdir /etc/ldap/ssl`.
2. Move the certificates created for the OpenLDAP server from the Certificate of Authority to the ssl subdirectory:
    a. `scp openldap_cert.pem user1@openldap.acmefinancial.com:\ldap\ssl`
    b. `scp openldap_privatekey.pem user1@openldap.acmefinancial.com:\ldap\ssl`
    c. `scp acmefinancial.com-CA.pem user1@openldap.acmefinancial.com:\ldap\ssl`
3. Install the CA certificate so that local applications can use the certificate when necessary:
    a. `cp acmefinancial.com-CA.pem /usr/share/ca-certificates/acmefinancial.com-CA.crt`
    b. Add *acmefinancial.com-CA.crt* to the end of the /etc/ca-certificates.conf file.
    c. Enter `sudo update-ca-certificates`.
4. Create a certificate information file called certinfo.ldif in /etc/ldap/ssl with the following contents:

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/ssl/acmefinancial.com-CA.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/ssl/openldap_cert.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/ssl/openldap_privatekey.pem
```

5. Set permissions and ownership on the certificate files so that the openLDAP user can read the key file:
    a. `sudo adduser openldap ssl-cert`
    b. `chgrp ssl-cert /etc/ldap/ssl/openldap_privatekey.pem`
    c. `chmod g+r /etc/ldap/ssl/openldap_privatekey.pem`
    d. `chmod o-r /etc/ssl/ldap/openldap_privatekey.pem`
    e. **chown root.ssl-cert /etc/ldap/ssl/openldap_privatekey.pem**
    f. **chown root.ssl-cert /etc/ldap/ssl/openldap_cert.pem**
    g. **chmod root.ssl-cert /etc/ldap/ssl**
6. Reconfigure slapd by running the following command
    a. **ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/ldap/ssl/certinfo.ldif**
    b. Restart slapd **by running service slapd restart**

StartTLS should now be enabled.

7. Enable LDAPS by adding `ldaps:/// to the SLAPD_SERVICES` line in the */etc/default/slapd* file:

```
# slapd normally serves ldap only on all TCP-ports 389. slapd can al
so
# service requests on TCP-port 636 (ldaps) and requests via unix
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
SLAPD_SERVICES="ldap:/// ldapi:/// ldaps:///"
```

    a. Go to the SLAPD_SERVICES line and add ldaps:/// as shown above.
    b. Enter **service slapd restart** to restart the OpenLDAP service.
8. Prepare the slapd client to use StartTLS:
    a. Create the /etc/ldap/ssl directory.
    b. Copy acmefinancial.com-CA.pem to /etc/ldap/ssl/ directory.
    c. Go to the client computer and edit /etc/ldap/ldap.conf.
    d. Comment out the previous TLS_CACERT entry and add a new one pointing to the location of your CA certificate.

```
# TLS certificates (needed for GnuTLS)
#TLS_CACERT     /etc/ssl/certs/ca-certificates.crt
TLS_CACERT      /etc/ldap/ssl/acmefinancial.com-CA.pem
```

2.5.7 Formatting Audit Logs

The file */etc/ldap/logs/auditlog.log* stores log entries destined for the Splunk indexer. Using the following scripts, the logs were formatted in such a way that enables the Splunk indexer to easily determine the start and end of each log event.

2.5.8 Script: /etc/ldap/logs/auditlogscript

```
#!/bin/bash
# Remove newlines, make file a single string and dump to auditlog.string
tr -s  '\n' ' ' < /etc/ldap/logs/auditlog.log > /etc/ldap/logs/auditlog.string
# Change every occurrence of #0 to just 0
sed -i -e 's/#0/0/g' /etc/ldap/logs/auditlog.string
# Remove spaces between attributes and their values
sed -i -e 's/: /:/g' /etc/ldap/logs/auditlog.string
#Additional formatting helpful in showing field separation
sed -i -e 's/ /;;/g' /etc/ldap/logs/auditlog.string
# Change # to newline making each line a unique openldap event and dump
# to auditlog.lines
tr -s '#' '\n' </etc/ldap/logs/auditlog.string> /etc/ldap/logs/auditlog.lines
#Additional formatting in removing unneeded lines
sed -i '/;;end;;/d' /etc/ldap/logs/auditlog.lines
# Empty previous contents of outlog.log
# outlog.log is effectively overwritten when script runs
cp /dev/null /etc/ldap/logs/outlog.log
# Call add-timestamp.py to add readable timestamps and dump to outlog.log
/etc/ldap/logs/add-timestamp.py
```

2.5.9 Script: /etc/ldap/logs/add-timestamp.py

```
#!/usr/bin/python3
import datetime
start_index = 0
end_index = 0
timestamp = 123456789  #var to store datetime object; values are placeholders
localtime = "12345"   #string var to store local time; values are placeholders
filename = "/etc/ldap/logs/auditlog.lines" #Each event in file is a line
#Open the file, parse each each line,identified char set in IF
#statement exposing the epoch_time without leading or trailing  chars
with open(filename, 'r') as file_object:
   for string in file_object:
      if ";;dc" in string:
         end_index = string.find(";;dc")
         string = string.strip()
         newstring = string[start_index:end_index]
         newstring = newstring.lstrip(';')
         newstring = newstring.lstrip('add')
         newstring = newstring.lstrip('modify')
         newstring = newstring.lstrip('delete')
         newstring = newstring.lstrip('rdn')
         newstring = newstring.lstrip(';')
         epoch_time = int(newstring)     #Store epoch_time as integer
         #Convert epoch_time to  datetime object and store in  timestamp
         timestamp = datetime.datetime.fromtimestamp(epoch_time)
         #Convert value in timestamp to string and store in localtime
         localtime = str(timestamp)
      #If line is blank, do nothing, else prepend localtime to line
      if string.isspace():
         pass
      else:
```

```
        with open('/etc/ldap/logs/outlog.log','a') as outfile_object:
          outfile_object.write(localtime + string + '\n')
```

2.5.10 Script: /etc/cron.daily/openldap-status

```
#!/bin/bash
#This script sends online status updates to splunk with enough information
#such that anlytics on Splunk can determine whether or not this host has
#failed to send updates in a given period.

if ls /var/log/oldstatustime # check if file exists
then
  prevtime=$(cat /var/log/oldstatustime) #store date in file in variable prevtime
else
  date >/var/log/oldstatustime  #else write current date to file path
fi
#write time hostname previous run time and online keyword to file path
#in a single line separated by commas
((date && hostname && echo $prevtime && echo online)|tr -s '\n' ','|sed
s'/online,/online/';echo "") >> /var/log/openldap-status-file.csv
date > /var/log/oldstatustime
```

2.6 Radiant Logic

Radiant Logic RadiantOne Virtual Directory Server (VDS) is a virtual directory that performs a federated identity service. (Note: Radiant Logic changed their product name from RadiantOne Virtual Directory Server (VDS) to RadiantOne Federated Identity Service (FID)).

2.6.1 How Its Used

The RadiantOne VDS (VD) is used in two capacities in this example implementation. First, the VD acts as a federated identity service, correlating users from each directory into a single view. Second, the VD acts as a monitoring service, where the created view is cached, and changes made to the cache are logged and sent to Splunk.

2.6.2 Virtual Machine Configuration

The Radiant Logic virtual machine is configured as follows:

- Ubuntu Linux 16.04 LTS
- 4 CPU cores
- 24GB of RAM
- 2 NICs
- 100GB of storage

Network Configuration (Interface 1)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.17.100
Netmask: 255.255.255.0
Gateway: 192.168.17.1

DNS Name Servers: 192.168.17.1
DNS-Search Domains: n/a

Network Configuration (Interface 2)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.14.111
Netmask: 255.255.255.0
Gateway: 192.168.14.1
DNS Name Servers 192.168.14.1
DNS-Search Domains: n/a

2.6.3 Installing the Virtual Directory

To install the VD, see the documentation provided with the software. The VD installation guide can also be found on the Radiant Logic support website here.

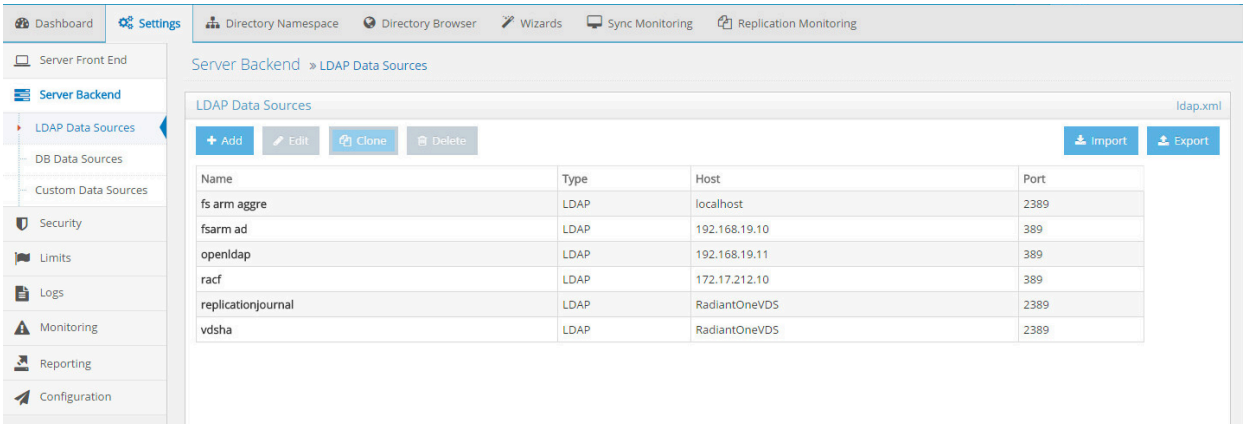
2.6.4 Configuring VD

Steps for configuring the VD are as follows:

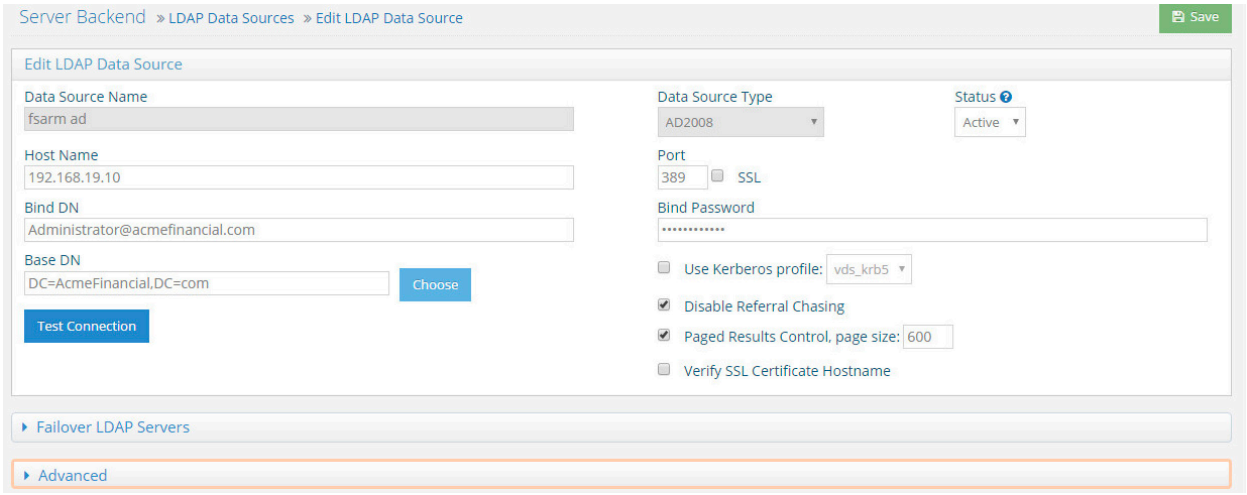
- Add server backends.
- Create proxy backend.
- Configure caching and system connectors.
- Create SharePoint view.
- Log Settings.

To add the server backends in the VD, complete the following steps:

1. While logged in as the Directory Manager, navigate to **Settings>Server Backend>LDAP Data Sources,**
2. Click **Add.**

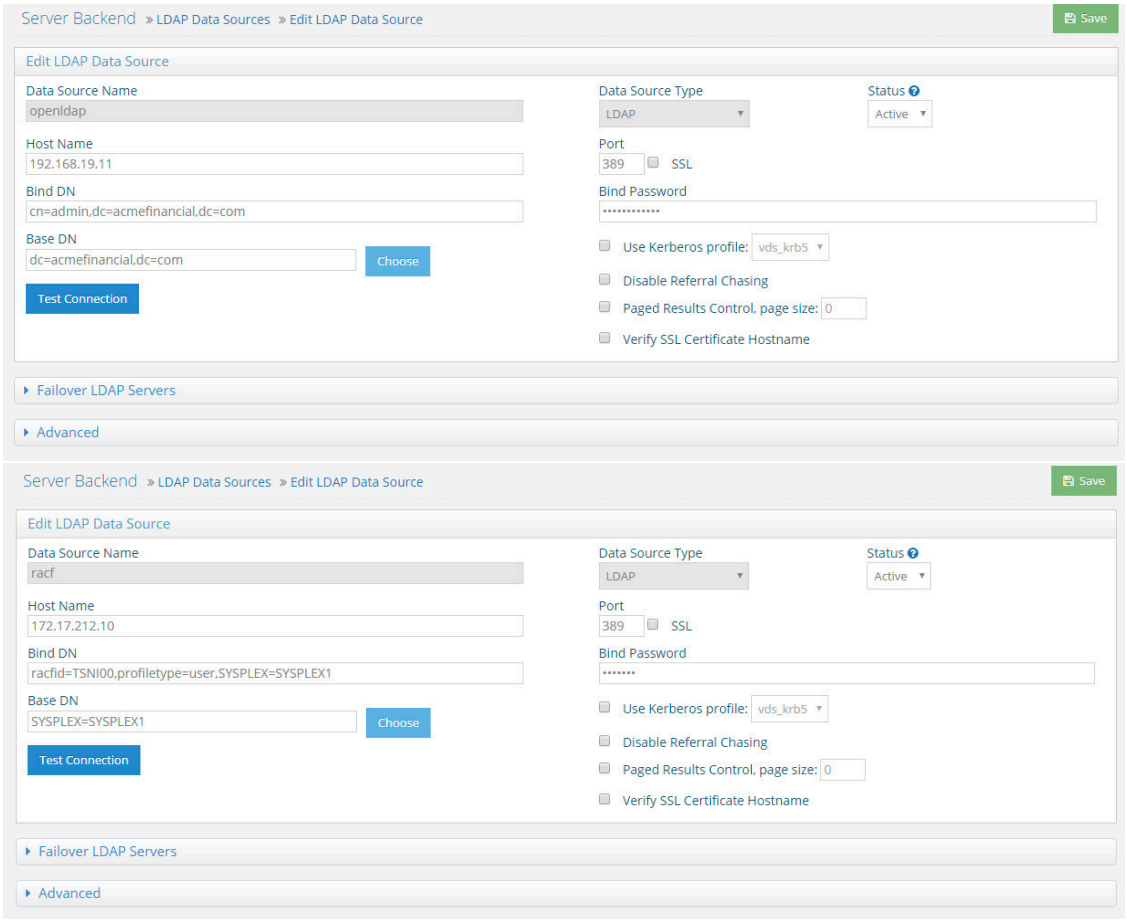


3. Name the data source and enter the parameters. For AD, the parameters used are shown in the following screenshot. Click **Save.**



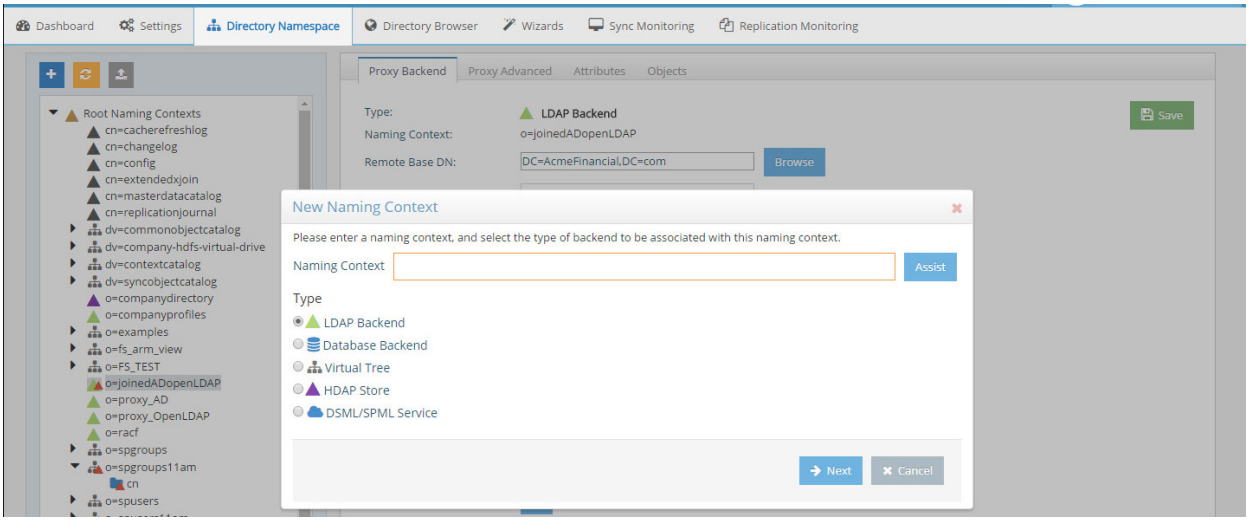
Note: Be sure to select **Disable Referral Chasing** for AD.

4. Repeat Steps 2 and 3 for the OpenLDAP and RACF directories. Use LDAP as the data source type. Details for each are shown in the following screenshots:

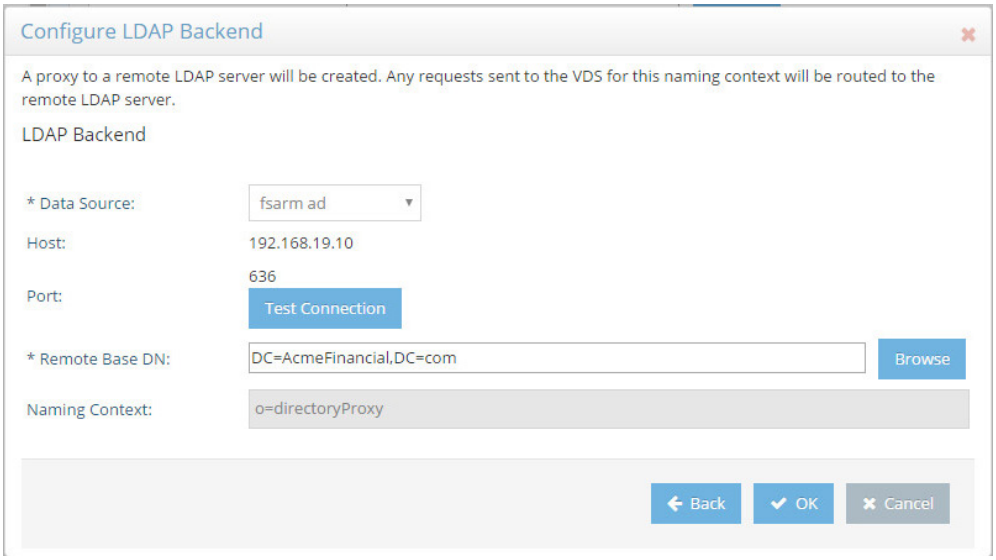


To create a proxy view to the backend directories, complete the following steps:

1. On the Directory Namespace tab, select **New Naming Context** (the plus sign) at the top left of the screen.
2. Select **the LDAP Backend** radio button and enter a naming context such as o=directoryProxy. Select **Next**.

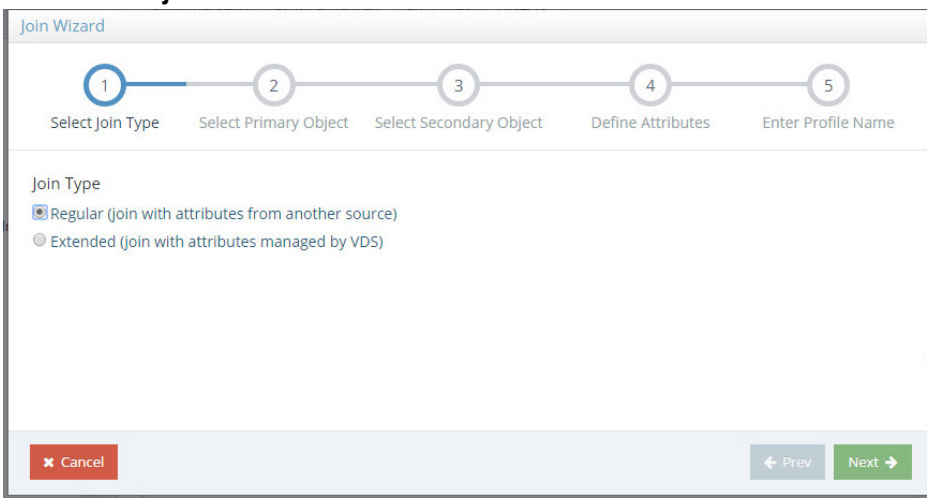


3. Select the name of the AD backend created earlier as the **Data Source**. Select the **Remote Base DN** of the domain. Select **OK.**

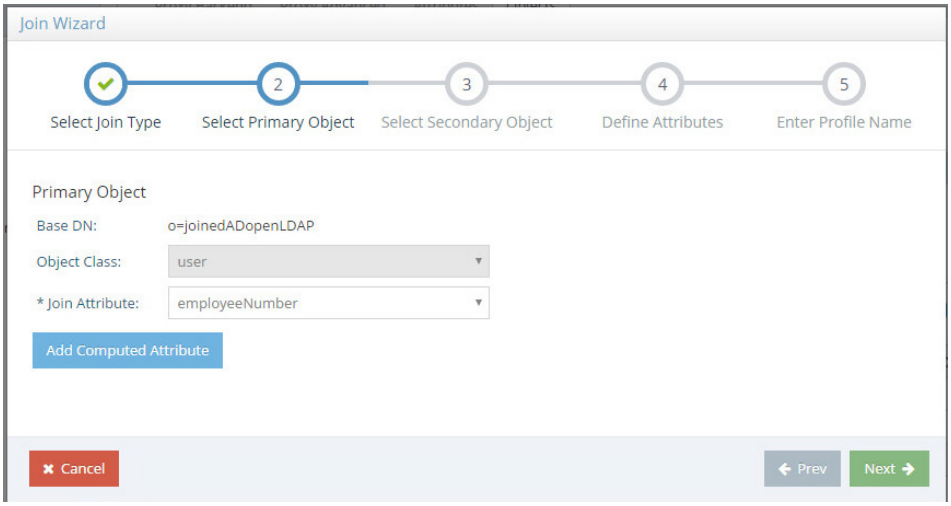


4. When the LDAP proxy is created, select the root naming context created in the left window pane.

5. Select the **Objects** Tab. Select **New** under **Join Profiles**.

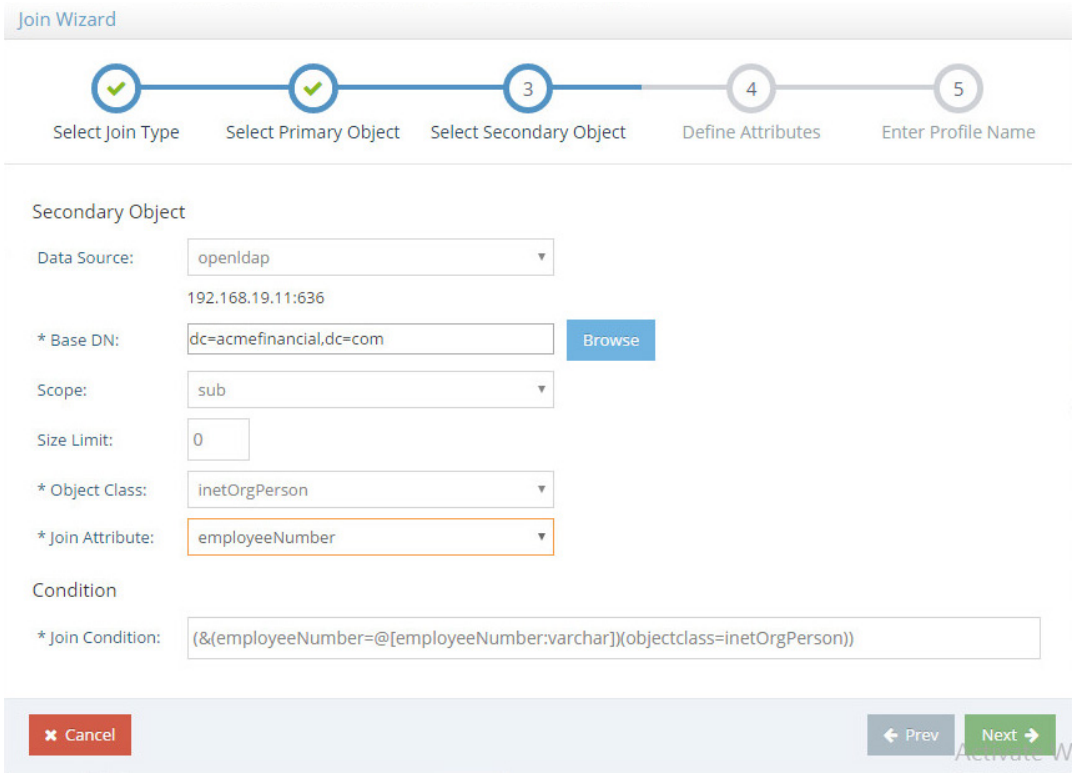


6. Choose **Regular.** Click **Next.**
7. Select employeeNumber as the Join Attribute. Click **Next**. *Note:* The employee number must be unique for each user. For example, if an employee has an account in AD and OpenLDAP, the



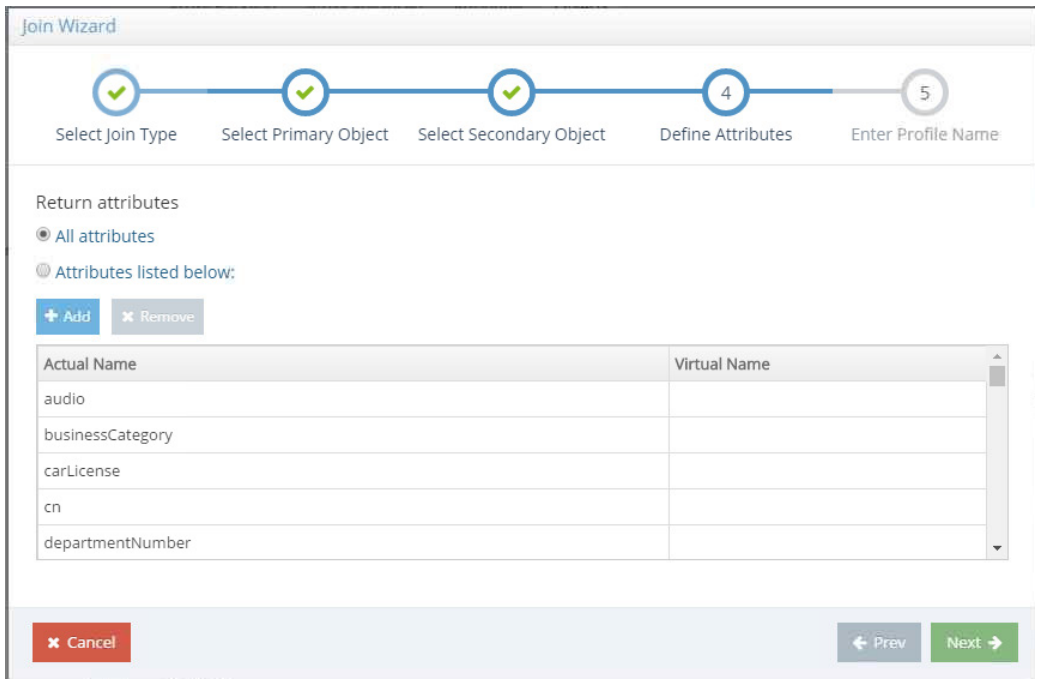
employeeNumber attribute should be the same in both sources for that employee.

8. Select **openLDAP** as the **Data Source** and enter **dc=acmefinancial,dc=com** as the **Base DN**. Specify **sub** as the **Scope**, **inetOrgPerson** as the **Object Class**, and **employeeNumber** as the **Join Attribute**. Leave **Size Limit** as default. Click **Next**.



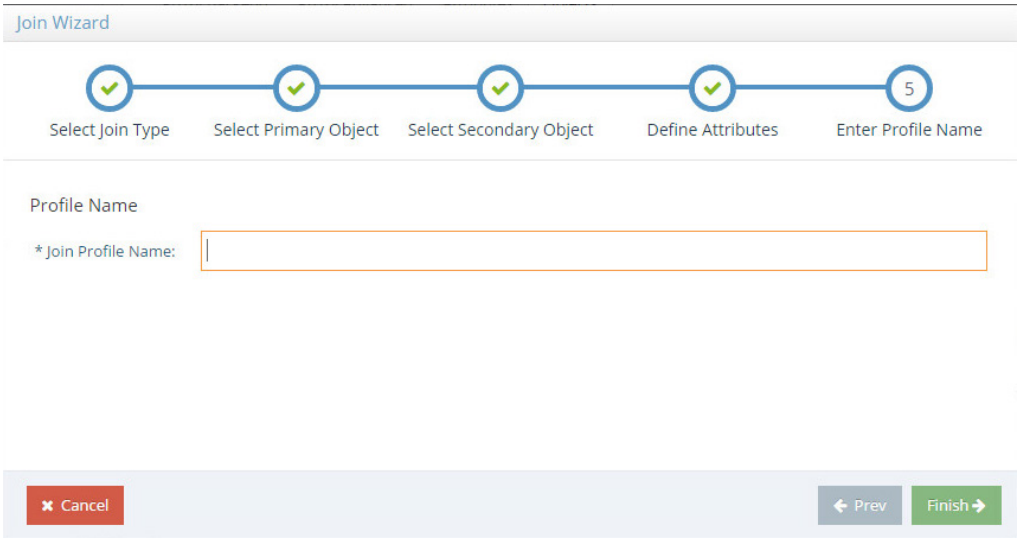
1497

1498 9. Select **All Attributes**. Click **Next.**



1499

10. Name the Join Profile. Click **Finish.**

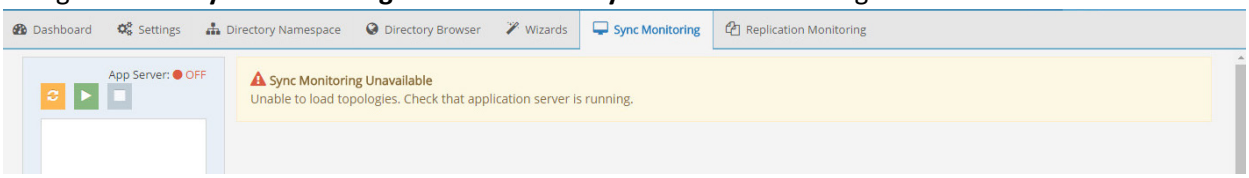


11. Repeat Steps 5–10 to join the RACF directory using the appropriate RACF objectClass and Base DN.

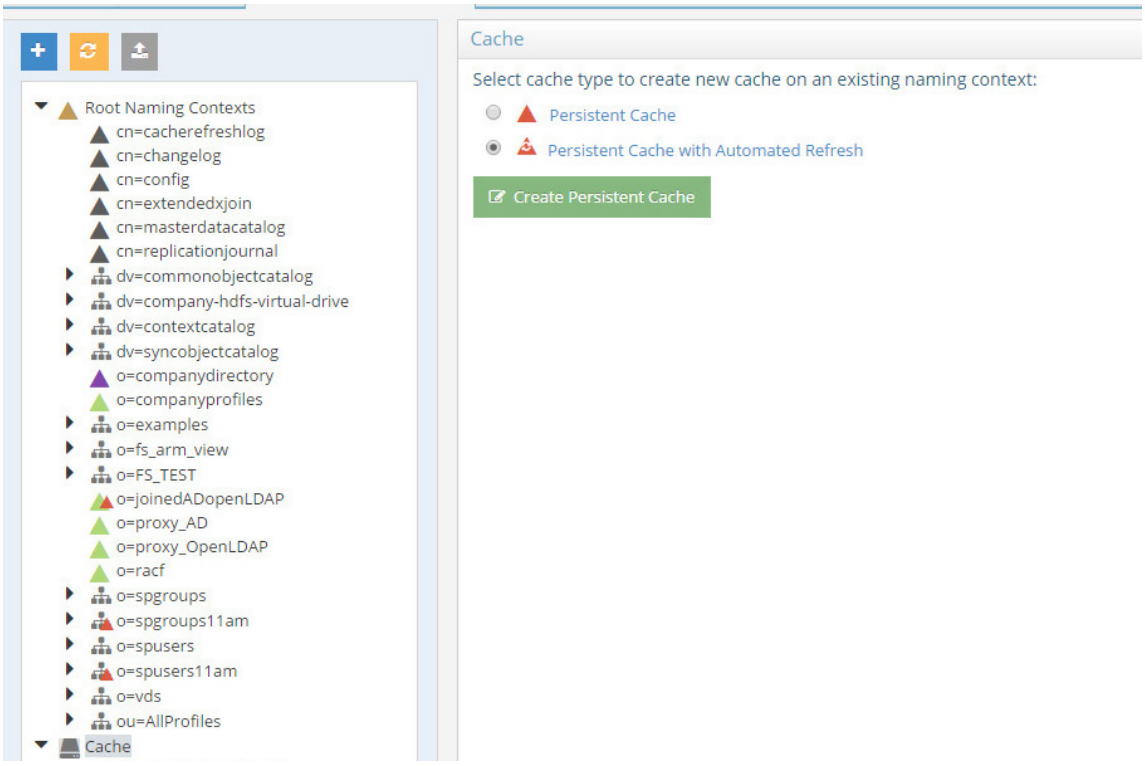
2.6.5 Configure Logging

To log changes to each directory object, you must create a cache for the proxy view created in the previous section. To create the cache and log changes made to the backend directories, complete the following steps:

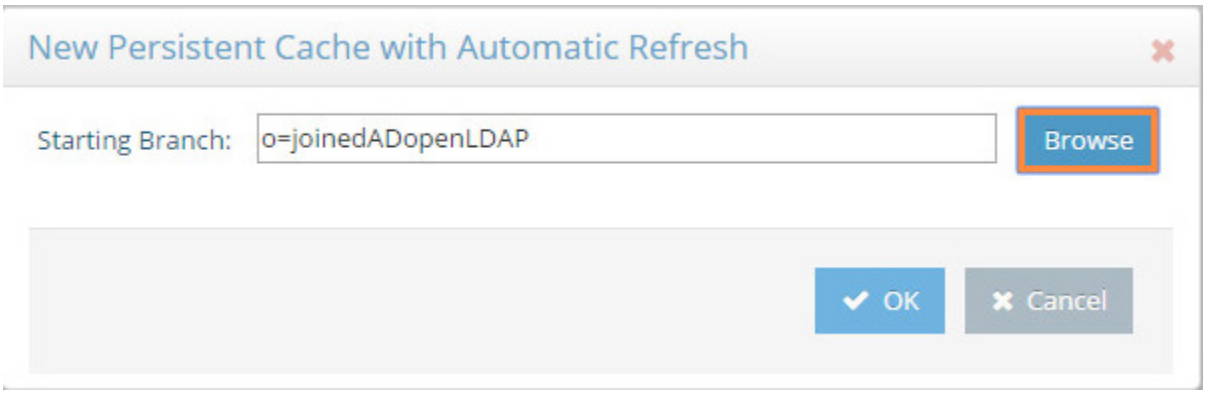
1. Navigate to the **Sync Monitoring** tab. Press the **Play** button to start the glassfish server.



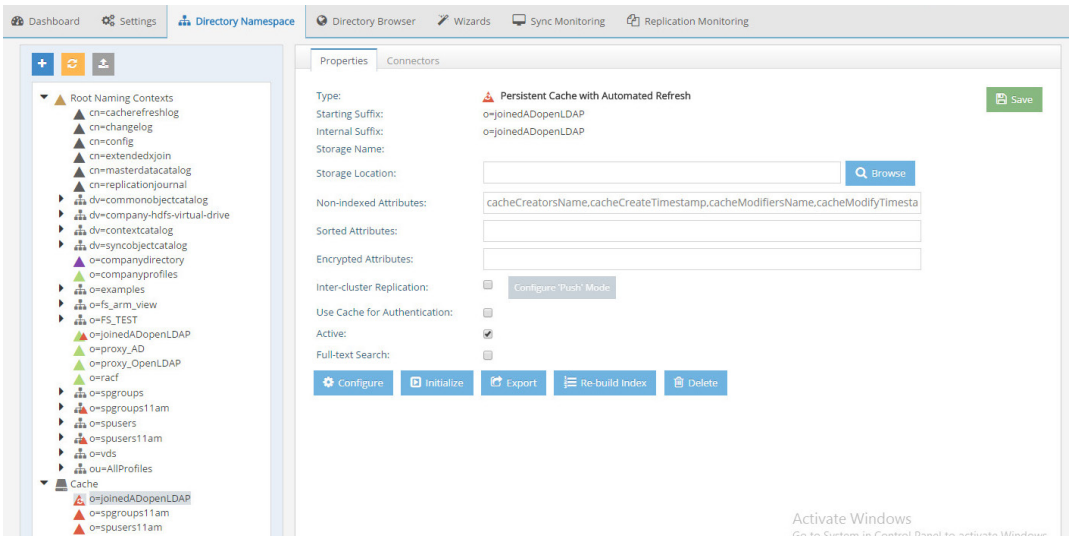
2. In the **Directory Namespace** tab, highlight **Cache** in the left window pane. Select **Persistent Cache with Automated Refresh**. Click **Create Persistent Cache.**



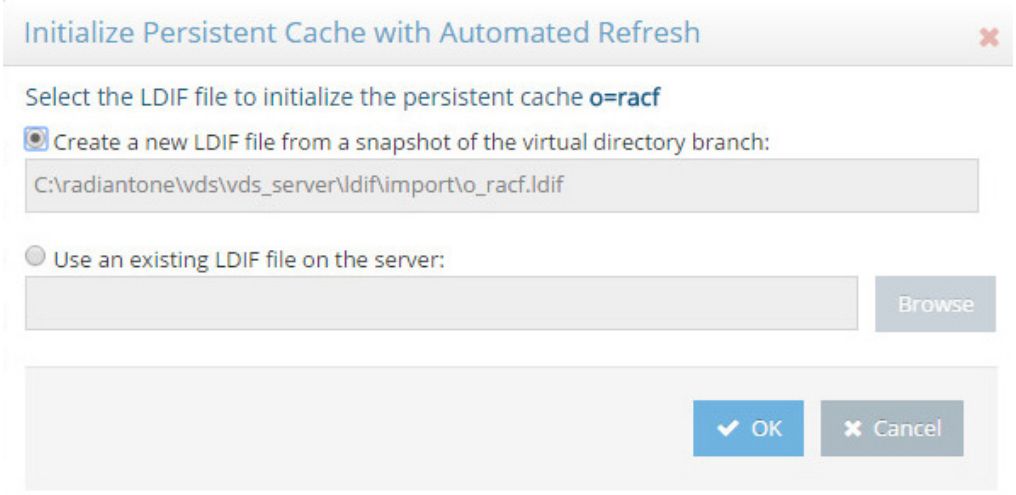
3. Browse and select the LDAP proxy created in the previous section. Select **OK.** The VD creates the cache.



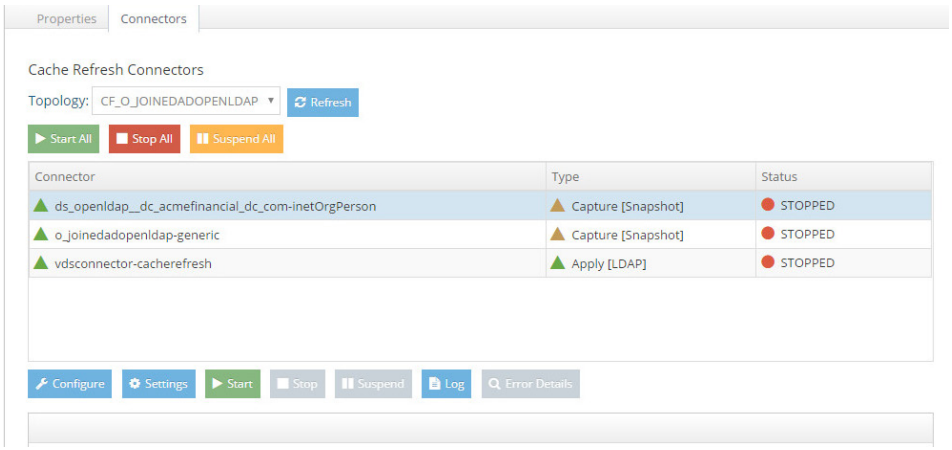
4. Select the created cache from the lower left window. Click **Initialize** to make the cache active.



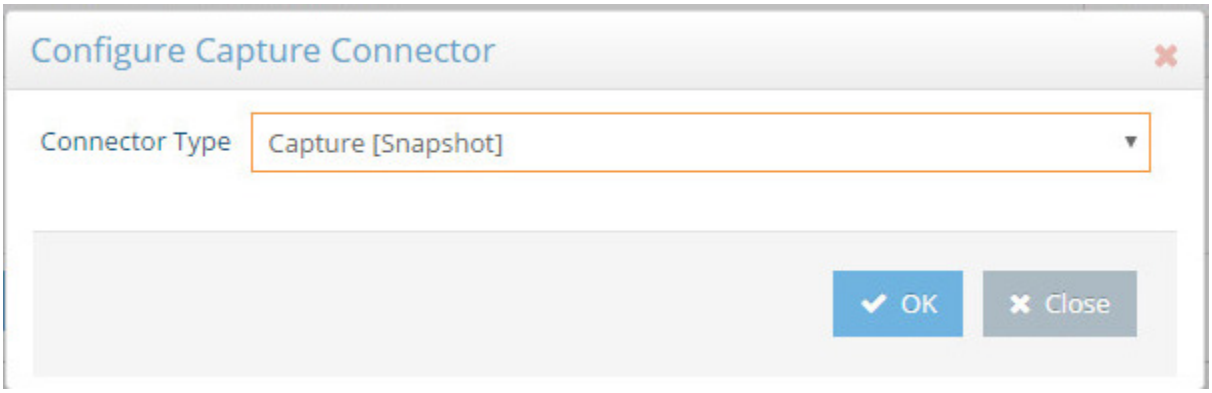
5. Select **Create a new LDIF file from a snapshot of the virtual directory branch**. Click **OK**. This step may take a while depending on the number of accounts in the backend directories.



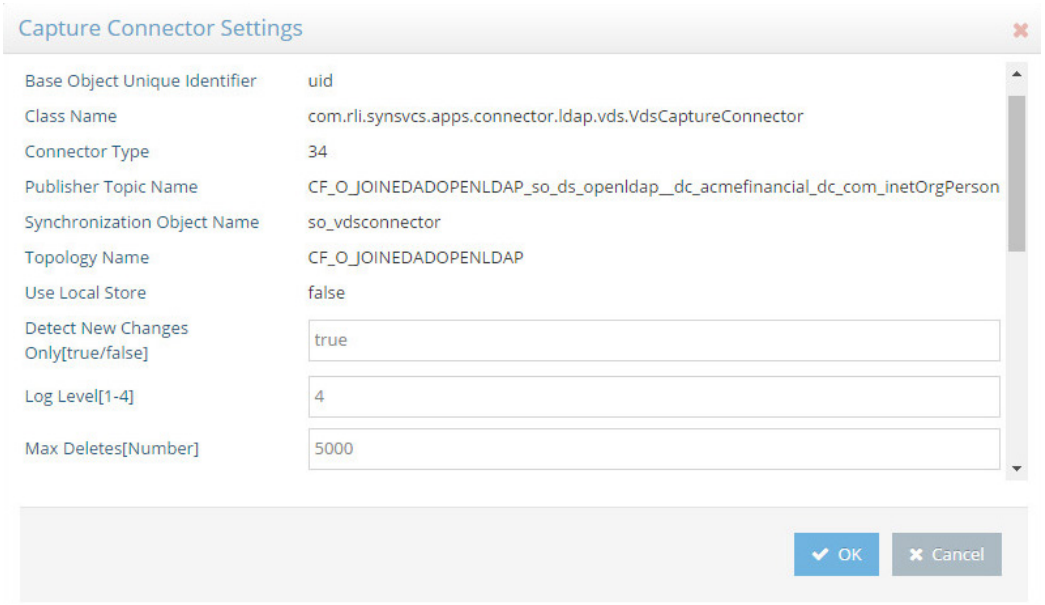
6. Once complete, **Save** the settings.
7. Select the **Connectors** tab.



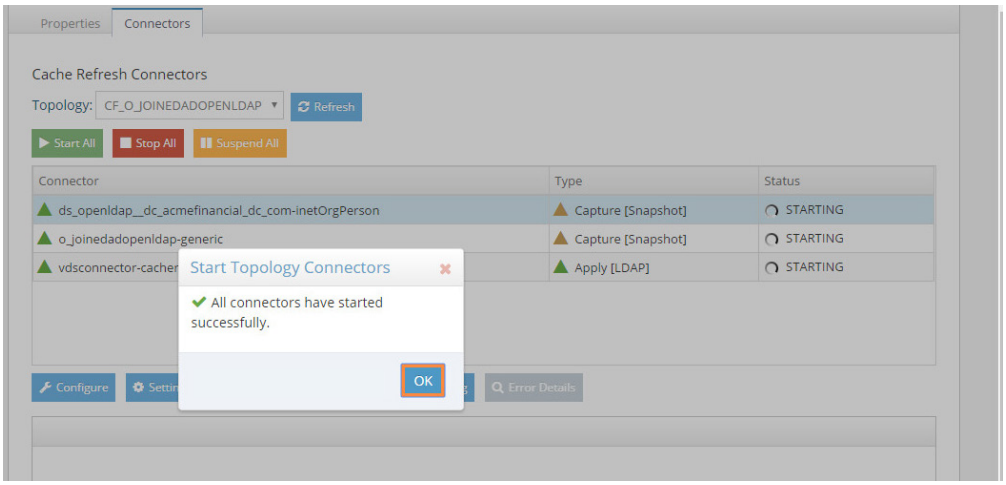
8. There should be a connector for each backend directory and one for the connector itself. Highlight the first connector. Select **Configure.** Change the connector type to "Capture [Snapshot]." Click **OK**. Repeat this step for each connector except the "vdsconnector-cacherefresh."



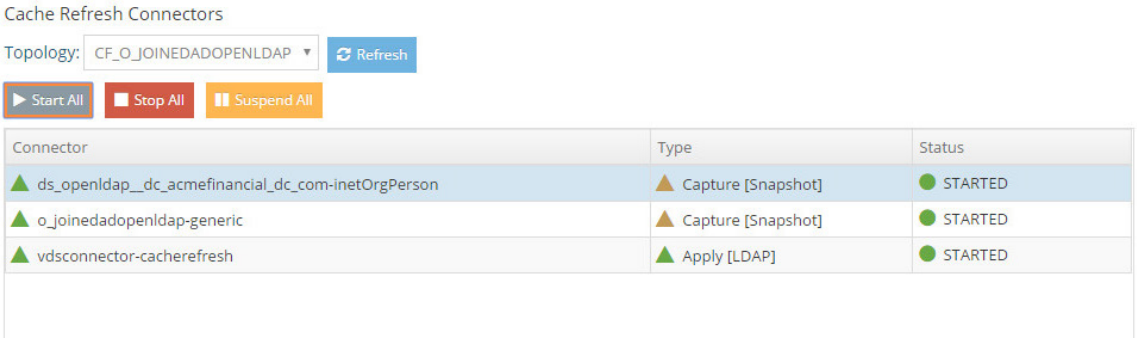
9. Back at the **Connectors** tab, highlight the first connector. Select **Settings**. Change the log level to the number 4. Click **OK**. Repeat this step for each connector except the "vdsconnector-cacherefresh."



10. Select **Start All** to start all the connectors. Click **OK**.



11. If the **Status** from each connector reads STARTED, you are done with this step. If not, review the logs and check the connections to the backend databases.

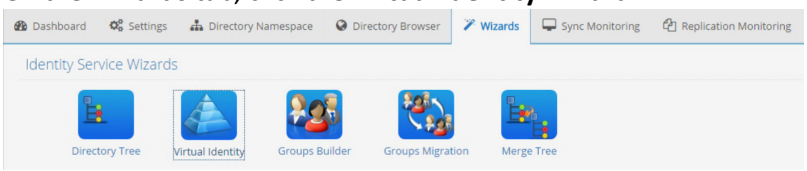


2.6.6 Configure Views for SharePoint

For applications to perform a global search (identify a user and locate groups) in the virtual namespace and be able to locate entries from many different types of underlying sources, the schemas must be mapped to a common naming context. There are many possible ways to configure virtual views for identities. We will leverage the Virtual Identity Wizard and the Groups Builder Wizard. For more details on each wizard, refer to the *RadiantOne System Admin Guide*. This guide is available on request.

To configure the Virtual Identities for SharePoint, follow these steps:

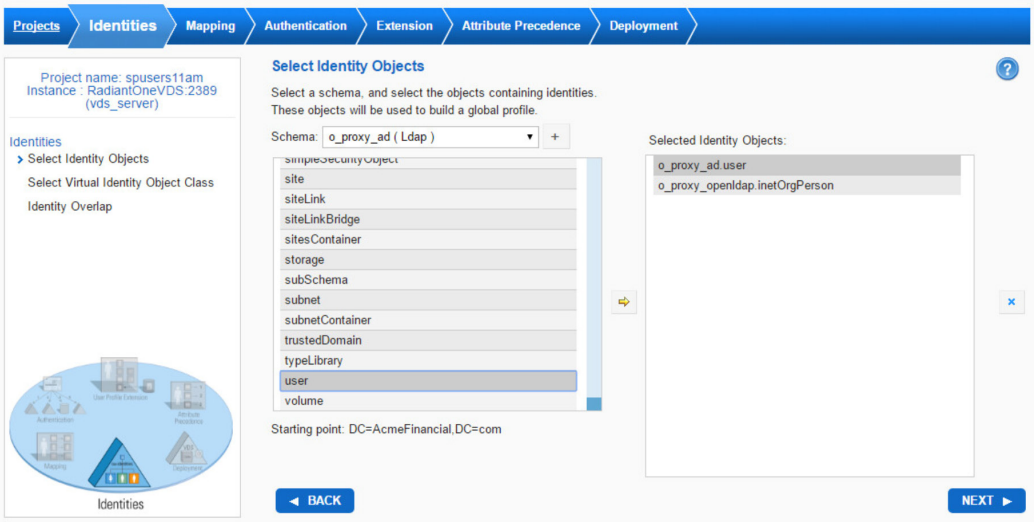
1. On the **Wizards** tab, click the **Virtual Identity Wizard**.



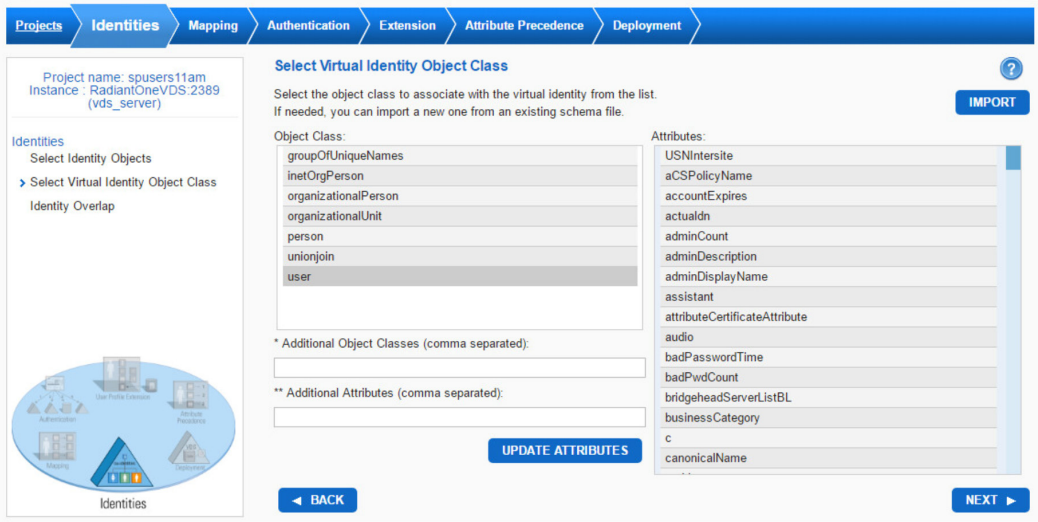
2. Click **Next**.
3. Click **New** and enter a project name (e.g., spusers) and click **Next**.
4. If you do not already have the schemas extracted from the data sources (or even data sources defined), use the + button to do so. The schema objects selected must be the ones associated with the user entries in the backends (e.g., InetOrgPerson for the LDAP, and user for AD). For more information, including exact steps on this process, see the *RadiantOne System Admin*

Guide.

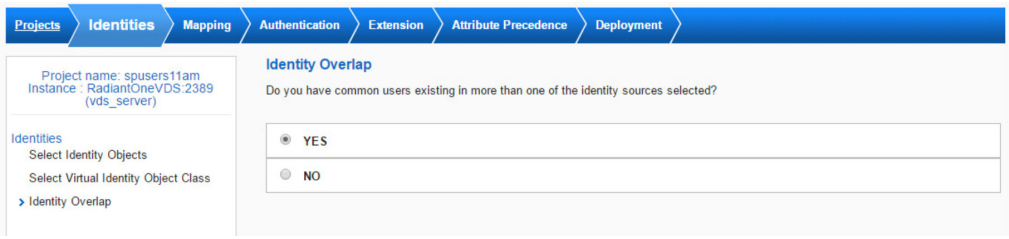
5. After connections to the backends are established and the schemas have been extracted, the drop-down list will be be populated with these objects. Select the object (e.g., objectclass) for each of the data sources and use the button to define it as a "Selected Identity Object."
6. Create the Selected identity objects shown below with the user schema from the AD backend and the inetOrgPerson from the openLDAP backend.



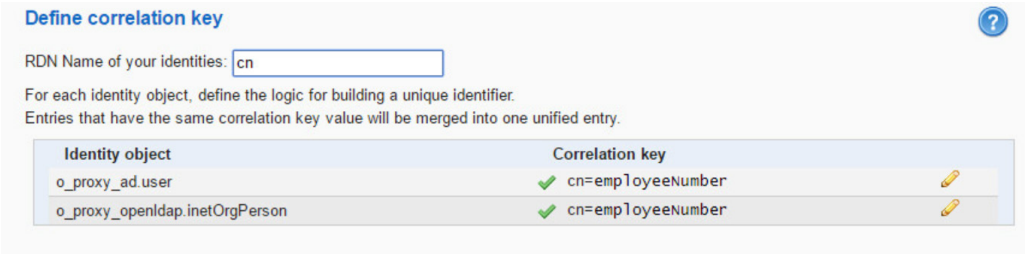
7. Click **Next**.
8. Select the objectclass to associate the virtual entries with. To support forms-based authentication in SharePoint via the LDAP Membership Provider, you should make sure that the objectclass you select here later matches the one used to configure the SharePoint web application's web.config file. The user object class is used here.



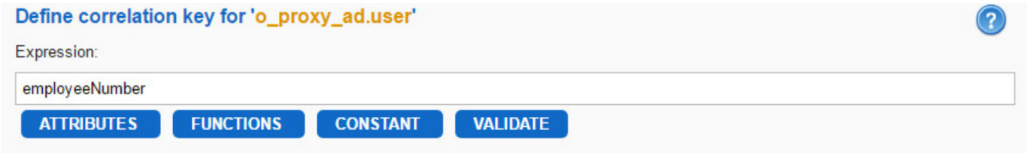
9. Click **Next**.
10. Select **Yes**. Click **Next**.



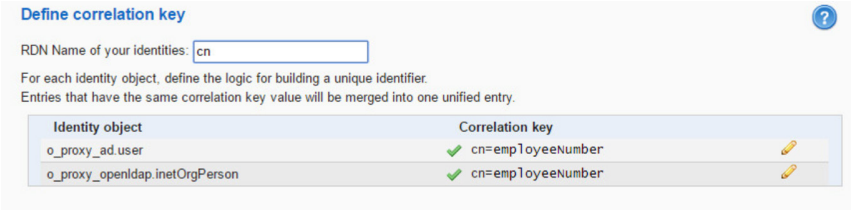
11. Define cn as the relative distingusihed name (RDN) Name of your identities.



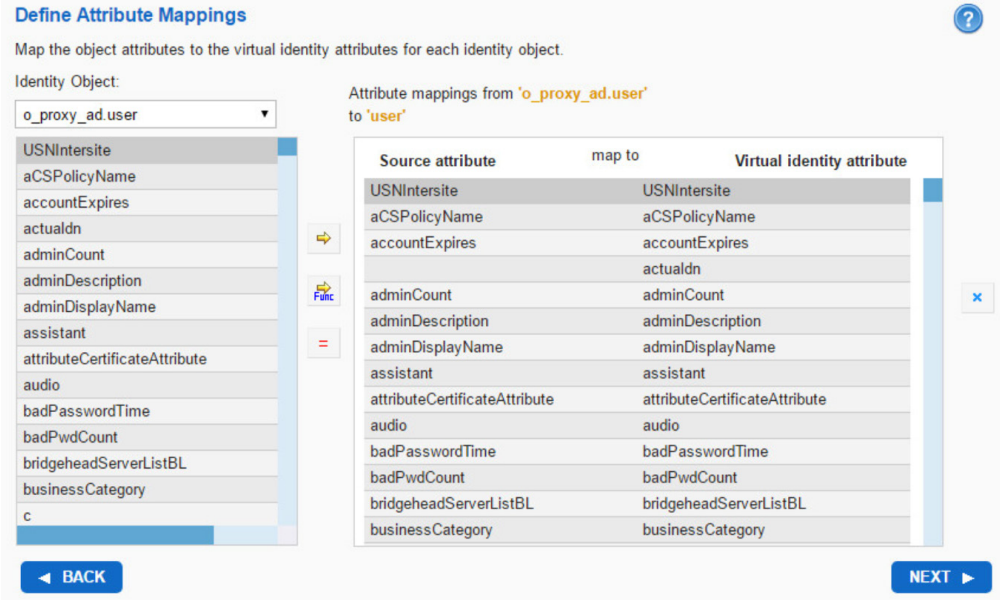
12. Select the button next to the user identity object. Set the correlation key as the employee number. Click **Next.**



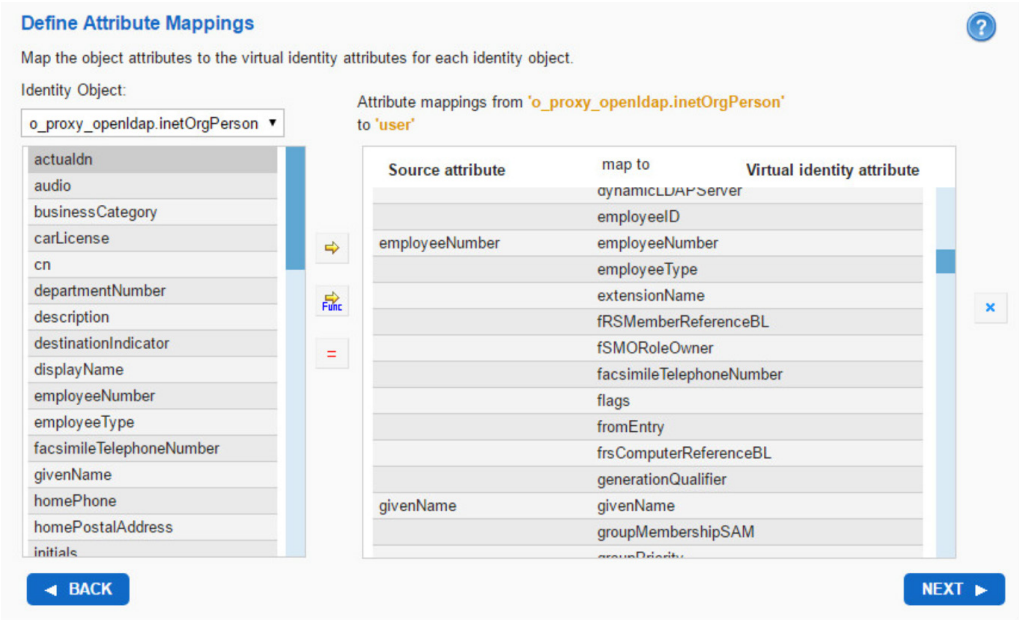
13. Repeat Step 12 for the inetOrgPerson identity object. Your correlation keys should have a green check to them as shown below. Click **Next**.



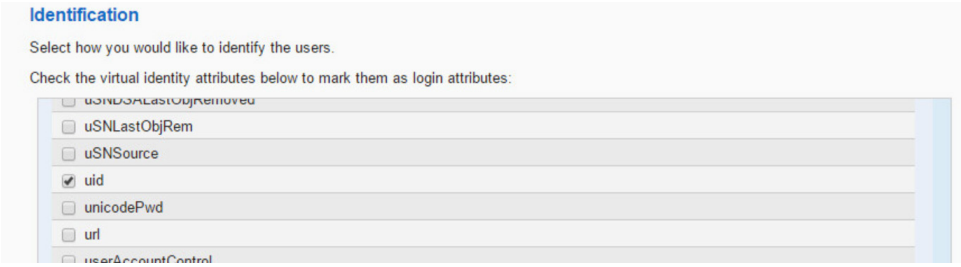
Here you define the attributes you want to return from each source. In this example, all attributes except **acutaldn** and **objectclass** are mapped from AD.



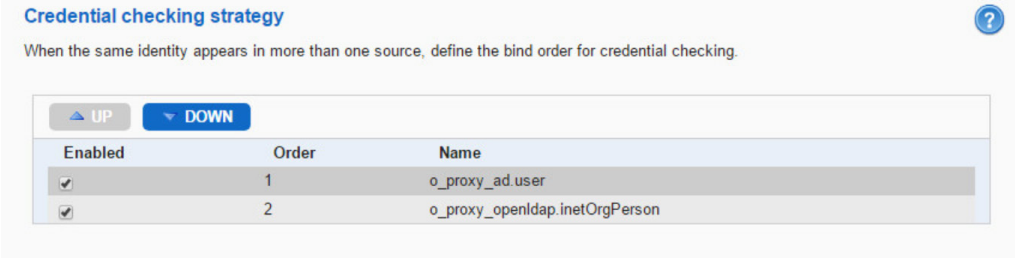
14. For OpenLDAP, note that employeeNumber, givenName, l, o, sn, and uid are mapped.



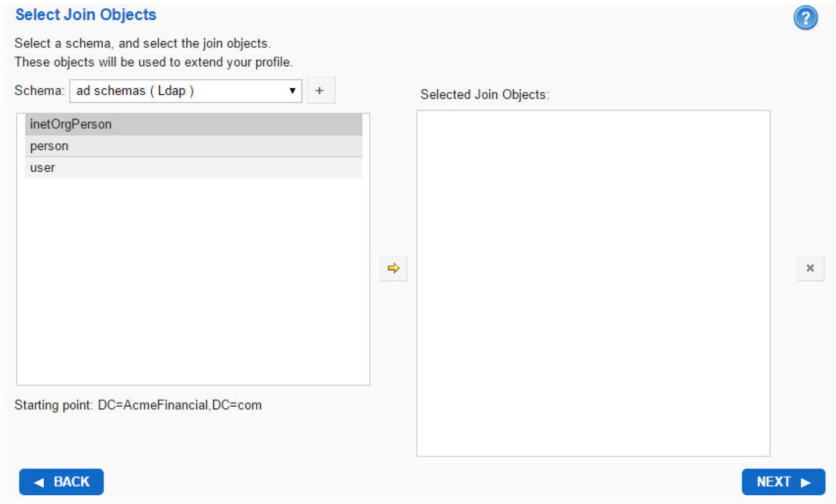
15. Select **Next** once the source attributes are mapped to the Virtual identity attribute.
16. Select the **uid** attribute as the identification attribute for user. The **uid** attribute contains the value that users will log in to SharePoint with. Select **Next**.



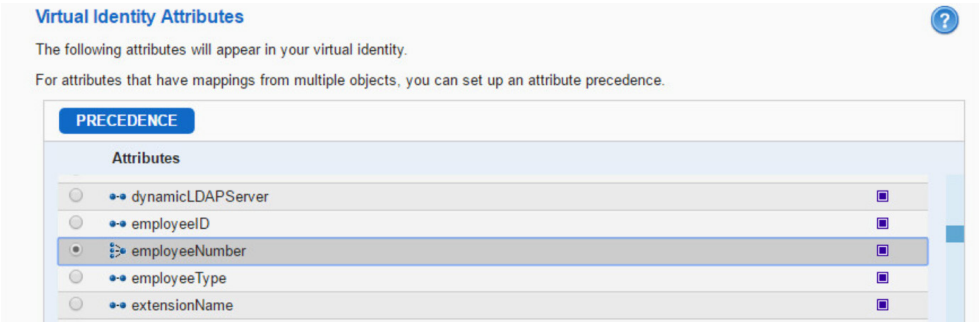
17. Enable both AD and OpenLDAP for credential checking. Give ADprecedence in the bind order. Click **Next**.



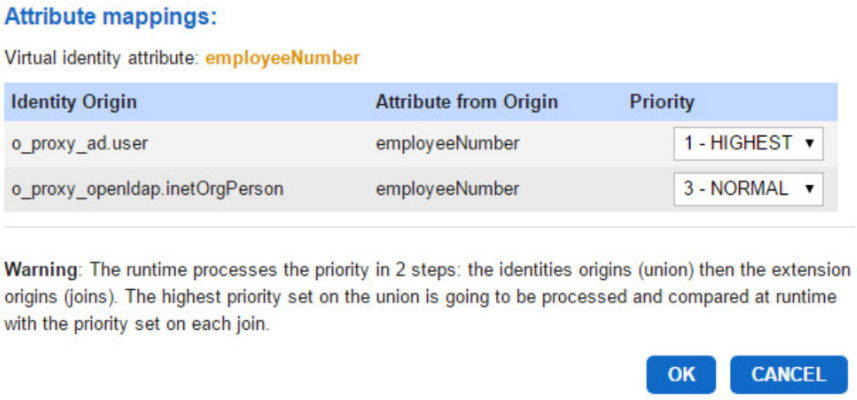
18. Do not select **Join Objects**. Click **Next**.



19. You can set each attribute precedence for any attributes that have mappings from multiple objects. Select the employeeNumber attribute. Click **PRECEDENCE**.

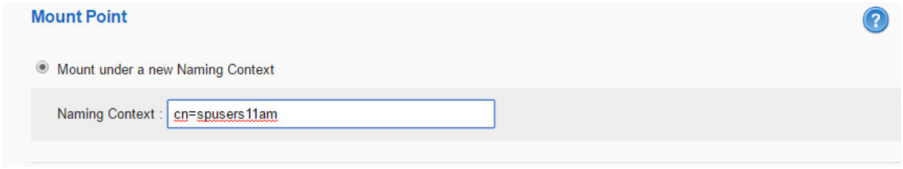


20. Give AD the highest priority. Click **O**

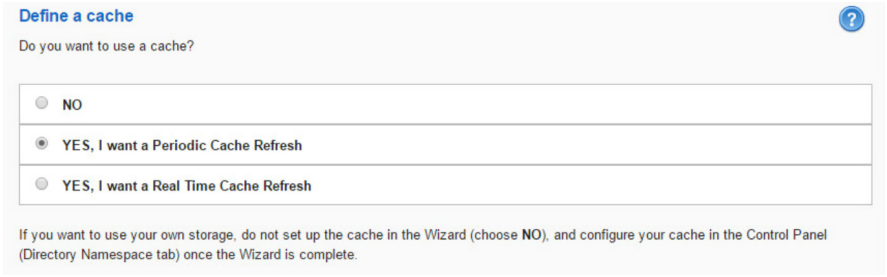


21. Click **Next**.

22. Name the naming context. For example, cn=spusers. Click **Next.**



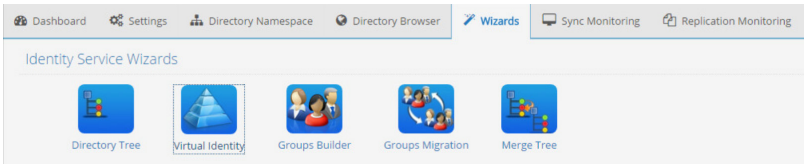
23. Select **Yes, I want a Periodic Cache Refresh**. Click **Next**.



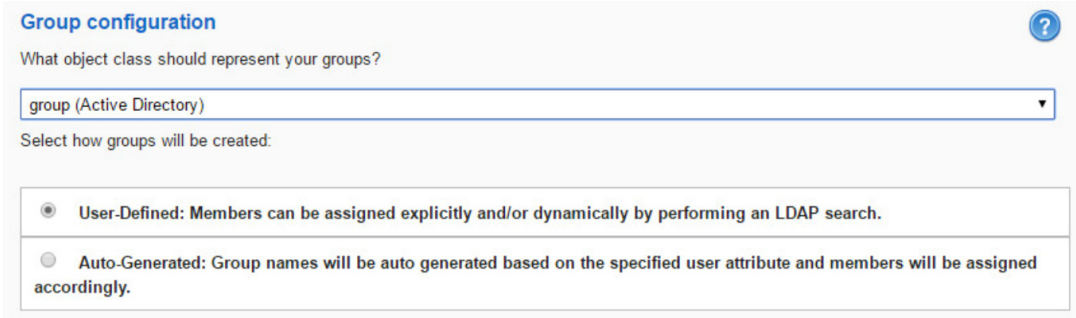
24. Define the refresh interval. Click **Next**.
25. Click **Initialize Cache Now**. Click **Finish**.

Follow these steps to configure the groups for SharePoint:

1. On the **Wizards** tab, click the **Groups Builder Wizard**.

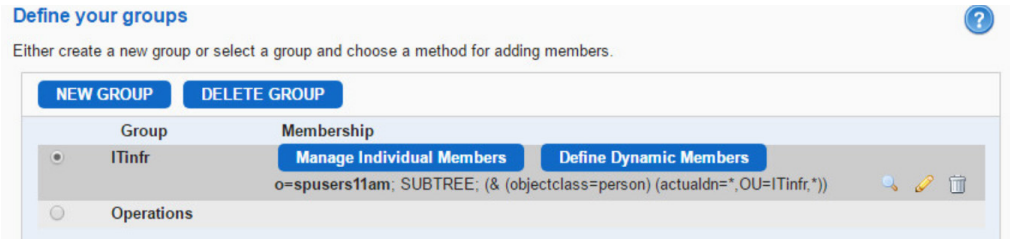


2. Click **Next**.
3. Name the project. Click **Next**.
4. From the drop-down menu select **group (Active Directory).** Select **User-Defined**. Click **Next**. For more information on user-defined and auto-generated group, see the *RadiantOne FID System Admin Guide*.

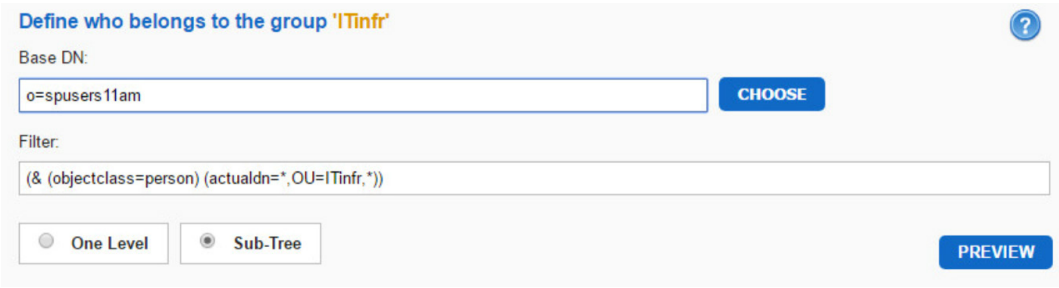


5. Select **New Group**. Name the group ITinfr. Click **Next**.

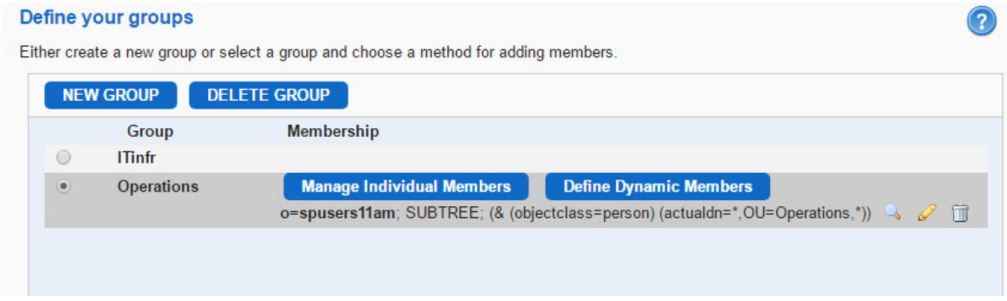
6. Repeat Step 5. Name the group Operations.
7. Select the first Group. Click **Define Dynamic Members.**



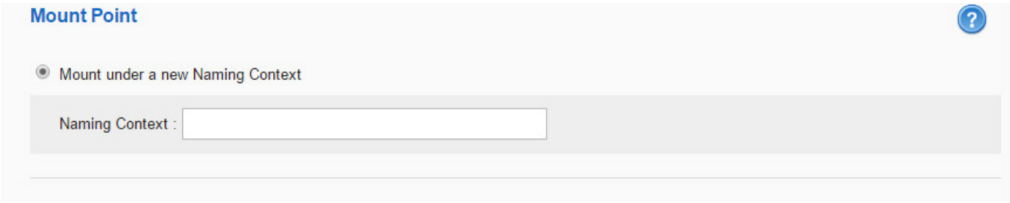
8. Choose the naming context created in Step 23 of using the Virtual Identity Wizard. Type in the following in the filter field: `(& (objectclass=person)(actualdn=*,OU=ITinfr,*))`. Select **Sub-Tree**. Click **Next**.



9. Repeat Steps 7 and 8 with the following filter: `(& (objectclass=person)(actualdn=*,OU=Operations,*))`.
10. Click **Next**.



11. Enter a naming context to mount under. For example, cn= spgroups. Click **Next**.



12. Select **Yes, I want a Periodic Cache Refresh**. Click **Next**.

13. Define the refresh interval. Click **Next**.
14. Click **Initialize Cache Now**. Click **Finish**.

2.6.7 Scripts

Two PowerShell scripts are scheduled to run on regular intervals on RadiantOne VDS server. The goal of these scripts is to determine if the virtual directory server (RadiantOne VDS) and the RACF directory server are online or offline. The first script determines if RadiantOne VDS is online or offline and writes the corresponding status message to a local file being monitored by Splunk. The second script, which also runs on the RadiantOne VDS server, determines if the Vanguard RACF directory is reachable and writes corresponding offline or online messages to a local file also being monitored by Splunk.

2.6.8 Script: RadiantOnlineStatus.ps1

```
#This script checks determines if this server is online or offline
#If gateway route exists and VDS server is running, the script will
#output the current time, hostname, status and previous time (last
#time it wrote to output file)
#Check if gateway route exists and if the VDS service is running
if ((Get-Netroute 0.0.0.0/0) -And (Get-Process vdsserver))
   {
   #Store date in PrevTime variable
   $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
   #Check if prevtime-file.txt exists
   if (ls C:\scripts\Radiant\prevtime-file.txt)
      {
         #Place the contents of prevtime-file.txt in the PrevTime variable
      $PrevTime=Get-Content C:\scripts\Radiant\prevtime-file.txt
      }
   #Place the current date in CurrentTime
   $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
   #Overwrite the contents of prevtime-file.txt with the current date
   Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\Radiant\prevtime-
file.txt
   $HostVar = hostname
   $Status = 'online'
   #Add the contents of the variables CurrentTime, HostVar, Status, PrevTime to
Radiant-Status-Output.csv
   Add-Content C:\scripts\Radiant\Radiant-Status-Output.csv
$CurrentTime','$HostVar','$Status','$PrevTime
   }
else
   {
   $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
   if (ls C:\scripts\Radiant\prevtime-file.txt)
      {
      $PrevTime=Get-Content C:\scripts\Radiant\prevtime-file.txt
      }
```

```
   $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
   Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\Radiant\prevtime-
file.txt
   $HostVar = hostname
   $Status = 'offline'
   Add-Content C:\scripts\Radiant\Radiant-Status-Output.csv
$CurrentTime','$HostVar','$Status','$PrevTime
   }
```

2.6.9 Script: VanguardOnlineStatus.ps1

```
#Script checks if the RACF mainframe is online and outputs status messages to file


#Check if the RACF mainframe is reachable with pings


if (ping -n 3 172.17.212.10 | select-string "Reply from 172.17.212.10")
   {
   #Store date in PrevTime variable
   $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
    #Check if prevtime-file.txt exists
   if (ls C:\scripts\Vanguard\prevtime-file.txt)
     {
        #Place the contents of prevtime-file.txt in the PrevTime variable
     $PrevTime=Get-Content C:\scripts\Vanguard\prevtime-file.txt
     }
   #Place the current date in CurrentTime
   $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
   #Overwrite the contents of prevtime-file.txt with the current date
   Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\Vanguard\prevtime-
file.txt
   $HostVar = "VanguardMainframe.acmefinancial.com"
   $Status = 'online'
   Add-Content C:\scripts\Vanguard\VanguardServer-Output.csv
$CurrentTime','$HostVar','$Status','$PrevTime
   }
else
   {
   $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
```

```
   if (ls C:\scripts\Vanguard\prevtime-file.txt)
      {
      $PrevTime=Get-Content C:\scripts\Vanguard\prevtime-file.txt
      }
   $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
   Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\Vanguard\prevtime-
file.txt
   $HostVar = "VanguardMainframe.acmefinancial.com"
   $Status = 'offline'
   Add-Content C:\scripts\Vanguard\VanguardServer-Output.csv
$CurrentTime','$HostVar','$Status','$PrevTime
   }
```

2.6.10 LDAPS Configuration

RadiantOne VDS virtual directory service connects to the Active Directory, OpenLDAP, and RACF backend directory servers and takes snapshots of the directory contents. Configuring LDAPS ensures that this process is encrypted with SSL. To use LDAPS to make these connections, follow these steps:

1. Copy the certificates of the backend directories to the RadiantOne VDS virtual directory server.
2. Import each certificate into the client trust store by opening the **Main Control Panel.**
3. Click **Settings** tab > **Security** section > **Client Certificate Trust Store.**
4. The certificates will be dynamically loaded into the Client Certificate Trust Store.
5. Configure the backend connections to use LDAPS by going to the **Settings** tab.
6. **Click Server Backend** > **LDAP Data Sources** > **Edit LDAP Data Source.**
7. Check the **SSL** box and type **636** into the **Por**t text box.

2.7 SharePoint

SharePoint is a web-based, collaborative platform. SharePoint is primarily used as a document management and storage system. It also supports workflow and applications.

2.7.1 How It's Used

SharePoint 2013 is used as the web application to demonstrate the capability of the Access Rights Management example solution.

2.7.2 Virtual Machine Configuration

The SharePoint virtual machine is configured as follows:

- Ubuntu Linux 16.04 LTS
- 4 CPU cores
- 32GB of RAM
- 2 NICs

- 120GB of storage

Network Configuration (Interface 1)
IPv4 Manual
IPv6 Disabled
IP Address: 192.168.17.113
Netmask: 255.255.255.0
Gateway: 192.168.17.1
DNS Name Servers: 192.168.19.10
DNS-Search Domains: acmefinancial.com

2.7.3 Prerequisites

See the Microsoft online documentation for hardware and software prerequisites.

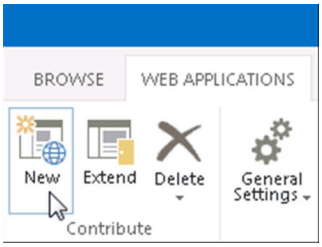
2.7.4 Installing SharePoint 2013

1. Installing SQL Server 2012: On the server where SharePoint 2013 is going to be installed, follow the steps from this link to install SQL Server 2012: https://technet.microsoft.com/en-us/library/ms143219(v=sql.110).aspx
2. Installing IIS on the SharePoint Server: On the server where SharePoint 2013 is going to be installed, follow the steps from this link to install IIS 8.0: http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012
3. Installing SharePoint Server 2013: On the server where SharePoint Server 2013 is going to be installed, follow the steps from this link to install SharePoint Server 2013: http://social.technet.microsoft.com/wiki/contents/articles/14209.sharepoint-2013-installation-step-by-step.aspx

2.7.5 Configuring SharePoint

SharePoint must be integrated with the Radiant Logic Virtual Directory using Forms-Based Authentication. To integrate with the VD, complete the following steps:

1. Open the SharePoint Central Administration Console, log in with your admin user, and click **Application Management**.
2. Below the **Web Applications** section, click on **Manage Web Applications**.

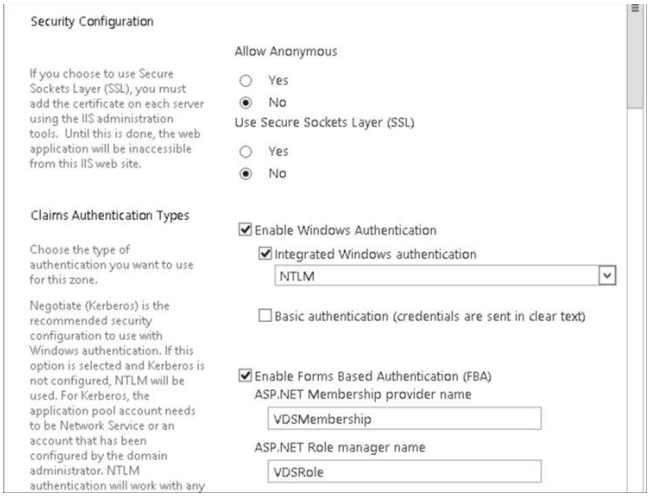


3. Click the **New** button.
4. You can choose to create a new IIS website and set a unique port.

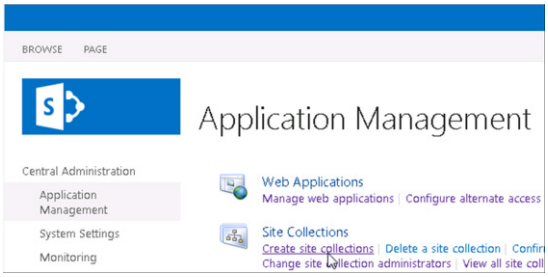
   Typically, you should accept the default path.

5. In the Security Configuration section, you can leave the default options (Allow Anonymous=No, Use SSL=No).

6. In the Claims Authentication Types section, check the option to **Enable Forms Based Authentication (FBA).**
7. Enter a unique name for the ASP.NET Membership provider name and ASP.NET Role manager name.

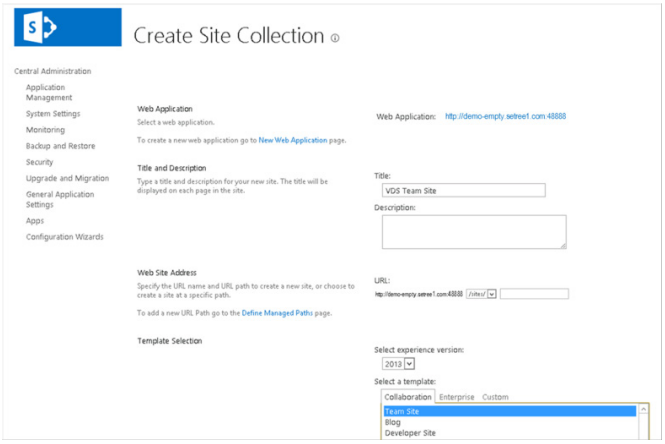


8. Leave the default sign-in page option selected.
9. In the Public URL section, leave the default URL and Zone.
10. In the Application Pool section, you can choose to “Create new application pool” and choose the “Predefined” option for the security account. Select the **Network Service** predefined option.
11. Leave the default values for the Database Name and Authentication, Failover Server, Search Server, Service Application Connections, and Customer Experience Improvement Program sections.
12. Click **OK** to create the new site.
13. Because this is a new site, you will also need to setup a Site Collection. In the Application Management section, click **Create Site Collections**.



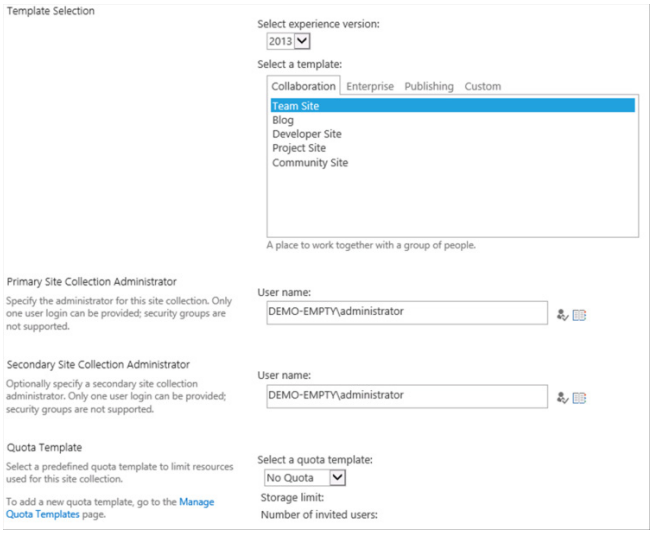
14. Make sure your application shows in the Web Application parameter (if not, click in the drop-down list to select a new one). Enter a title description and web site address and choose a template.

1798



1799

1800 15. Enter a primary and secondary site collection Administrator. Click **OK.**



1801

1802 2.7.6 Web Configs

1803 Three web config files must be edited to complete the integration with Radiant Logic.

1804 SharePoint STS web config file is located at *C:\Program Files\Common Files\Microsoft Shared\Web*
1805 *Server Extensions\15\WebServices\SecurityToken*.

1806 The web.config file has a default membership provider and a default role provider. Do not change them.
1807 The names of the new membership provider and role manager that get added into the web.config file
1808 must match the names set in the Forms Based configuration for the web application.

1809 Modify the file to include the following xml code in the <system.web> section.

```
1810 <system.web>
1811 <membership defaultProvider="i">
1812 <providers>
1813 <clear/>
```

```
<add name="i"
type="Microsoft.Sharepoint.Administration.Claims.SPClaimsAuthMembershipProvider,
Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c" />

<add name="VDSMembership"
type="Microsoft.Office.Server.Security.LdapMembershipProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"

       server="192.168.14.111"

       port="2389"

       useSSL="false"

       connectionUsername="cn=Directory Manager"

       connectionPassword="Fsarm@nccoe1"

       useDNAttribute="false"

       userDNAttribute="distinguishedName"

       userNameAttribute="uid"

       userContainer="o=spusers11am"

       userObjectClass="user"

       userFilter="(ObjectClass=user)"

       scope="Subtree"

       otherRequiredUserAttributes="sn,givenname,cn,employeeNumber"/>

</providers>

</membership>

<roleManager defaultProvider="c" enabled="true" cacheRolesInCookie="false" >

<providers>

<clear/>

<add name="c"
type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthRoleProvider,
Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c" />

<add name="VDSRole"

type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
Version=15.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"

       server="192.168.14.111"

       port="2389"

       useSSL="false"

       groupContainer="o=spgroups11am"

       groupNameAttribute="cn"
```

```
        groupNameAlternateSearchAttribute="cn"
        groupMemberAttribute="member"
        userNameAttribute="uid"
        useUserDNAttribute="false"
        userContainer="o=spusers11am"
        dnAttribute="distinguishedName"
        groupFilter="(ObjectClass=group)"
        userFilter="(ObjectClass=user)"
        scope="Subtree" />
</providers>
</roleManager>
</system.web>
```

SharePoint Central Admin web config file is located at *C:\inetpub\wwwroot\wss\VirtualDirectories\<port the central admin is on>*.

There is a default membership provider and a default role provider in the web.config file. Do not change them. The names of the new membership provider and role manager that get added into the web.config file must match the names set in the Forms Based configuration for the web application.

Modify the file to include the following xml code in the <system.web> section:

```
<membership defaultProvider="i">
<providers>
<clear />
<add name="i"
type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthMembershipProvider,
Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c" />
<add name="VDSMembership"
type="Microsoft.Office.Server.Security.LdapMembershipProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
        server="192.168.14.111"
        port="2389"
        useSSL="false"
        connectionUsername="cn=Directory Manager"
        connectionPassword="Fsarm@nccoe1"
        useDNAttribute="false"
        userDNAttribute="distinguishedName"
```

```
        userNameAttribute="uid"
        userContainer="o=spusers11am"
        userObjectClass="user"
        userFilter="(ObjectClass=user)"
        scope="Subtree"
        otherRequiredUserAttributes="sn,givenname,cn,employeeNumber"/>
</providers>
</membership>
<roleManager defaultProvider="c" enabled="true" cacheRolesInCookie="false">
<providers>
<clear />
<add name="c"
type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthRoleProvider,
Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c" />
<add name="VDSRole"
type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
Version=15.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
        server="192.168.14.111"
        port="2389"
        useSSL="false"
        groupContainer="o=spgroups11am"
        groupNameAttribute="cn"
        groupNameAlternateSearchAttribute="cn"
        groupMemberAttribute="member"
        userNameAttribute="uid"
        useUserDNAttribute="false"
        userContainer="o=spusers11am"
        cacheDurationInMinutes="0"
        dnAttribute="distinguishedName"
        groupFilter="(ObjectClass=group)"
        userFilter="(ObjectClass=user)"
        scope="Subtree" />
</providers>
</roleManager>
```

SharePoint Web Application web config is located at *C:\inetpub\wwwroot\wss\VirtualDirectories\<port the application is on>*.

There is a default membership provider and a default role provider in the web.config file. Do not change them. The names of the new membership provider and role manager that get added into the web.config file must match the names set in the Forms Based configuration for the web application.

Modify the file to include the following xml code in the <system.web> section:

```
<roleManager enabled=”true” defaultProvider=”AspNetWindowsTokenRoleProvider”
<providers>
<add name="VDSRole"
type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
       server="192.168.14.111"
       port="2389"
       useSSL="false"
       groupContainer="o=spgroups11am"
       groupNameAttribute="cn"
       groupNameAlternateSearchAttribute="cn"
       groupMemberAttribute="member"
       userNameAttribute="uid"
       dnAttribute="distinguishedName"
       groupFilter="(ObjectClass=group)"
       userFilter="(ObjectClass=person)"
       scope="Subtree" />
</providers>
</roleManager>
<membership>
<providers>
<add name="VDSMembership"
type="Microsoft.Office.Server.Security.LdapMembershipProvider,
Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c"
       server="192.168.14.111"
       port="2389"
       useSSL="false"
```

```
        connectionUsername="cn=Directory Manager"
        connectionPassword="Fsarm@nccoe1"
        useDNAttribute="false"
        userDNAttribute="distinguishedName"
        userNameAttribute="uid"
        userContainer="o=spusers11am"
        userObjectClass="person"
        userFilter="(ObjectClass=person)"
        scope="Subtree"
        otherRequiredUserAttributes="sn,givenname,cn"/>
</providers>
</membership>
</system.web>
```

To leverage RadiantOne Federated Identity for the SharePoint people picker, add the following line in the <PeoplePickerWildcards> section of the web.config files for the SharePoint site and the Central Admin (where VDSMembership is the name of the custom membership provider used):

```
<add key=”VDSMembership” value=”*” />
<PeoplePickerWildcards> <clear />
<add key="AspNetSqlMembershipProvider" value="%" />
<add key="VDSMembership" value="*" /> </PeoplePickerWildcards>
```

2.8 Splunk

Splunk is a Security Information and Event Management system that allows for the collection and parsing of logs and data from multiple systems.

2.8.1 How It’s Used

Splunk can receive data from a plethora of different sources. The most reliable option is installing Splunk’s “Universal Forwarder” on each system you want to collect data from. Other options include syslogs, file and directory monitoring, network events, and more. Once data has been collected by Splunk, it can then be parsed and displayed using prebuilt rules or custom criteria.

2.8.2 Installation

Note: You will need a Splunk account to download Splunk Enterprise. The account is free and can be set up at https://www.splunk.com/page/sign_up.

Download Splunk Enterprise from https://www.splunk.com/en_us/download/splunk-enterprise.html. Splunk can be installed on Windows, Linux, Solaris, and Mac OS X. Each of these installation instructions can be found at:

- Windows

- GUI: http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonWindows
- Command line: http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonWindowsviathecommandline

- Linux: http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonLinux
- Solaris: http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonSolaris
- Mac OS X: http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonMacOS

2.8.3 Queries

Splunk reports, alerts, and dashboards are powered by queries written in the Splunk Search Processing Language (SPL). These queries are used to perform the analytics responsible for capturing events, identifying trends, and detecting anomalies. Once a query is written, it can be saved as a report, an alert, or as a dashboard panel. The following queries were also saved to dashboards to provide a central viewing location for operators, managers, and decision makers.

2.8.4 Query: Detect User Provisioning Accounts Events

The following search query detects when a user account is provisioned or when the user account attributes are modified. The provisioning and modification events detected include those that are in compliance with the established workflow and originate from the approved provisioning system, as well as those that violate the workflow. The output of the query shows which events were authorized and which were not.

```
(index=main sourcetype="wineventlog:security" EventCode=5136 OR EventCode=4720) OR
(index=sandbox sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest") OR
(index=main sourcetype="openldap-outlog")|rex "givenName:(?P<FirstName>\w+)"|rex
"sn:(?P<LastName>\w+)"|rex mode=sed "s/;;/ /g"|rex
"changetype:(?P<RLICHANGETYPE>\w+)"|rex "employeeNumber:(?P<EmployeeNumber>\w+)"|rex
"changetype:modify (?P<CHANGE>.+)"|rex "conn=\d+\s\w+\:cn=(?P<LDAP_UID>\w+\S\w+)"|rex
"A user account was (?P<RLICHANGETYPE>\w+)"|rex "A directory service object was
(?P<RLICHANGETYPE>\w+)"|eval
RLICHANGETYPE=if(RLICHANGETYPE=="modified","update",RLICHANGETYPE)|eval
RLICHANGETYPE=if(RLICHANGETYPE=="created","insert", RLICHANGETYPE)|eval
RLICHANGETYPE=if(RLICHANGETYPE=="add","insert",RLICHANGETYPE)|fields _time host
checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
RLICHANGETYPE employeeNumber givenName sn uid gidnumber RLICHANGES LDAP_UID LDAP_MSG
AD_UID AD_MSG |rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex "\-create\(\):User:
(?P<AD_UID>\w+\s)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.\w+\s\w+\s\w+)"|rex "\-
create\(\):User: (?P<AD_MSG>\w+\s\w+\s\w+)" |rex
"<RLICHANGETYPE>(?P<RLICHANGETYPE>\w+)"|rex
"<RLICHANGES>(?P<RLICHANGES>.+)\<\/RLICHANGES\>"|rex "employeeNumber:
(?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
(?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\S+)"|rex
"departmentNumber: (?P<DeptNumber>\w+)"|rex "## l: (?P<L>\w+)"|rex "## o:
(?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
"mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\S+\s*\S+)"|rex
"\<givenName\>(?P<GivenName>\S+\s*\S+)\<\/givenName\>"|rex
"\<sn\>(?P<SurName>\S+\s*\S+)\<\/sn\>" |rex
"\<employeeNumber\>(?P<EmployeeNumber>\S+\s*\S+)\<\/employeeNumber\>" |table _time
```

```
host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
RLICHANGETYPE RLICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
LDAPUserId |where (isnotnull(FirstName)) OR (isnotnull(RLICHANGES) OR
(isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG))) OR isnotnull(RLICHANGETYPE)|eval
F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID) |table
_time host checkStatus EmpNo F_Name L_Name RLICHANGETYPE RLICHANGES checkAuthFields
LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLICHANGES=if(RLICHANGETYPE=="insert","New User
Record",RLICHANGES)| eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
host2=if(Like(host, "%WIN%"),"AlertE","NULL")|eval Authority=if((host1=="RadiantOne
VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
|table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
AD_UID ADCHANGETYPE|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE
RLICHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority !="Not Legal"|eval
CHANGES=if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
CHANGETYPE=if(isnotnull(RLICHANGETYPE),RLICHANGETYPE,RLICHANGETYPE)|table _time host
Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Not
Like(CHANGES, "%lastLogonTimestamp%")
```

2.8.5 Query: Authorized and Unauthorized Provisioning Trend Line Chart

The following search query generates a line chart showing the trends for both the authorized and unauthorized provisioning events:

```
earliest="1/25/2017:00:00:00" latest="2/15/2017:00:00:00" index=sandbox
sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest"|fields _time host
checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
RLICHANGETYPE employeeNumber givenName sn uid gidnumber RLICHANGES LDAP_UID LDAP_MSG
AD_UID AD_MSG|rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex "\-create\(\):User:
(?P<AD_UID>\w+\s)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.\w+\s\w+\s\w+)"|rex "\-
create\(\):User: (?P<AD_MSG>\w+\s\w+\s\w+)" |rex
"<RLICHANGETYPE>(?P<RLICHANGETYPE>\w+)"|rex
"<RLICHANGES>(?P<RLICHANGES>.+)\<\/RLICHANGES\>"|rex "employeeNumber:
(?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
(?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\S+)"|rex
"departmentNumber: (?P<DeptNumber>\w+)"|rex "## l: (?P<L>\w+)"|rex "## o:
(?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
"mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\S+\s*\S+)"|rex
"\<givenName\>(?P<GivenName>\S+\s*\S+)\<\/givenName\>"|rex
"\<sn\>(?P<SurName>\S+\s*\S+)\<\/sn\>" |rex
"\<employeeNumber\>(?P<EmployeeNumber>\S+\s*\S+)\<\/employeeNumber\>" |table _time
host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
RLICHANGETYPE RLICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
LDAPUserId|where (isnotnull(FirstName)) OR (isnotnull(RLICHANGES) OR
(isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG)))|eval
F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID) |table
```

```
_time host checkStatus EmpNo F_Name L_Name RLICHANGETYPE RLICHANGES checkAuthFields
LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLICHANGES=if(RLICHANGETYPE=="insert","New User
Record",RLICHANGES)| eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
host2=if(Like(host, "%WIN%"),"AlertE","NULL")|eval Authority=if((host1=="RadiantOne
VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
|table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
AD_UID|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE RLICHANGES
EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority !="Not Legal"|eval
CHANGES=if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
CHANGETYPE=if(isnotnull(RLICHANGETYPE),RLICHANGETYPE,RLICHANGETYPE)|table _time host
Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|timechart span=2d
count BY Authority
```

2.8.6 Query: Combined Provisioning Trend Line Chart

The following search query generates a line chart that shows the total authorized and unauthorized provisioning events combined in a single trend line:

```
index=sandbox sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest"|fields
_time host checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId
LDAPUserId  RLICHANGETYPE employeeNumber givenName sn uid gidnumber RLICHANGES
LDAP_UID LDAP_MSG AD_UID AD_MSG|rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex
"\-create\(\):User: (?P<AD_UID>\w+\s)"|rex "\-create\(\):User:
(?P<LDAP_MSG>\w+\.\w+\s\w+\s\w+)"|rex "\-create\(\):User: (?P<AD_MSG>\w+\s\w+\s\w+)"
|rex "<RLICHANGETYPE>(?P<RLICHANGETYPE>\w+)"|rex
"<RLICHANGES>(?P<RLICHANGES>.+)\<\/RLICHANGES\>"|rex "employeeNumber:
(?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
(?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\S+)"|rex
"departmentNumber: (?P<DeptNumber>\w+)"|rex "## l: (?P<L>\w+)"|rex "## o:
(?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
"mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\S+\s*\S+)"|rex
"\<givenName\>(?P<GivenName>\S+\s*\S+)\<\/givenName\>"|rex
"\<sn\>(?P<SurName>\S+\s*\S+)\<\/sn\>" |rex
"\<employeeNumber\>(?P<EmployeeNumber>\S+\s*\S+)\<\/employeeNumber\>" |table _time
host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
RLICHANGETYPE RLICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
LDAPUserId|where (isnotnull(FirstName)) OR (isnotnull(RLICHANGES) OR
(isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG)))|eval
F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID) |table
_time host checkStatus EmpNo F_Name L_Name RLICHANGETYPE RLICHANGES checkAuthFields
LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLICHANGES=if(RLICHANGETYPE=="insert","New User
Record",RLICHANGES)| eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
```

```
RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
host2=if(Like(host, "%WIN%"),"AlertE","NULL")|eval Authority=if((host1=="RadiantOne
VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
|table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
AD_UID|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE RLICHANGES
EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority !="Not Legal"|eval
CHANGES=if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
CHANGETYPE=if(isnotnull(RLICHANGETYPE),RLICHANGETYPE,RLICHANGETYPE)|table _time host
Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID |eval
Event=if(isnotnull(Authority),"Provisioning", "Null")|timechart span=2d count BY Event
```

2.8.7 Query: Detect modifications to High Value or Privileged Accounts

The following search query detects any modification to high-value accounts or privileged accounts, such as managers and system administrators. It detects modifications that violate corporate policy as well as those that are performed in accordance to policy.

```
(index=main sourcetype="wineventlog:security" EventCode=5136 OR EventCode=4720) OR
(index=sandbox sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest") OR
(index=main sourcetype="openldap-outlog")|rex "givenName:(?P<FirstName>\w+)"|rex
"sn:(?P<LastName>\w+)"|rex mode=sed "s/;;/ /g"|rex
"changetype:(?P<RLICHANGETYPE>\w+)"|rex "employeeNumber:(?P<EmployeeNumber>\w+)"|rex
"changetype:modify (?P<CHANGE>.+)"|rex "conn=\d+\s\w+\:cn=(?P<LDAP_UID>\w+\S\w+)"|rex
"A user account was (?P<RLICHANGETYPE>\w+)"|rex "A directory service object was
(?P<RLICHANGETYPE>\w+)"|eval
RLICHANGETYPE=if(RLICHANGETYPE=="modified","update",RLICHANGETYPE)|eval
RLICHANGETYPE=if(RLICHANGETYPE=="created","insert", RLICHANGETYPE)|eval
RLICHANGETYPE=if(RLICHANGETYPE=="add","insert",RLICHANGETYPE)|fields _time host
checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
RLICHANGETYPE employeeNumber givenName sn uid gidnumber RLICHANGES LDAP_UID LDAP_MSG
AD_UID AD_MSG |rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex "\-create\(\):User:
(?P<AD_UID>\w+\s)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.\w+\s\w+\s\w+)"|rex "\-
create\(\):User: (?P<AD_MSG>\w+\s\w+\s\w+)" |rex
"<RLICHANGETYPE>(?P<RLICHANGETYPE>\w+)"|rex
"<RLICHANGES>(?P<RLICHANGES>.+)\<\/RLICHANGES\>"|rex "employeeNumber:
(?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
(?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\S+)"|rex
"departmentNumber: (?P<DeptNumber>\w+)"|rex "## l: (?P<L>\w+)"|rex "## o:
(?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
"mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\S+\s*\S+)"|rex
"\<givenName\>(?P<GivenName>\S+\s*\S+)\<\/givenName\>"|rex
"\<sn\>(?P<SurName>\S+\s*\S+)\<\/sn\>" |rex
"\<employeeNumber\>(?P<EmployeeNumber>\S+\s*\S+)\<\/employeeNumber\>" |table _time
host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
RLICHANGETYPE RLICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
LDAPUserId |where (isnotnull(FirstName)) OR (isnotnull(RLICHANGES) OR
(isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG))) OR isnotnull(RLICHANGETYPE)|eval
F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID) |table
_time host checkStatus EmpNo F_Name L_Name RLICHANGETYPE RLICHANGES checkAuthFields
LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLICHANGES=if(RLICHANGETYPE=="insert","New User
Record",RLICHANGES)| eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
```

```
AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
host2=if(Like(host, "%WIN%"),"AlertE","NULL")|eval Authority=if((host1=="RadiantOne
VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
|table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
AD_UID ADCHANGETYPE|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE
RLICHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority !="Not Legal"|eval
CHANGES=if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
CHANGETYPE=if(isnotnull(RLICHANGETYPE),RLICHANGETYPE,RLICHANGETYPE)|table _time host
Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Not
Like(CHANGES, "%lastLogonTimestamp%")|table _time host Authority CHANGETYPE CHANGES
EmpNo F_Name L_Name LDAP_UID AD_UID|where isnotnull(CHANGETYPE) AND ((Like(CHANGES,
"%MNGR%")) OR (Like(CHANGES, "%Manager%") OR Like(CHANGES, "%Administrator%")))
```

2.8.8 Query: Virtual Directory Server Offline Detection

The following search query detects when the virtual directory server goes offline. The virtual directory server is configured to send online status messages to Splunk at regular intervals. This query searches for those messages and declares the virtual directory server offline if the last online message received has exceeded the expected interval.

```
earliest=-24h sourcetype="radiant-status"|table _time CurrentTime Hostname Status|sort
1 -_time|eval SearchTime_Epoch=now()|eval CTime_Epoch=strptime(CurrentTime,"%a %b %d
%H:%M:%S %Z %Y")|eval TimeDiff=(SearchTime_Epoch - CTime_Epoch)|eval Status=if(TimeDiff
> 900, "Offline", Status)|where Status=="offline"|table CurrentTime Hostname Status
```

2.8.9 Query: Critical Servers Offline

The following search query detects when a directory server goes offline. The query uses the results of multiple data sources to determine when a server is offline and when it is online.

```
earliest=-12h (index=sandbox sourcetype="radiantsourcetest" ERROR) OR (index=main
sourcetype=openldap-status1) OR (index=main sourcetype=AD-Status) OR
(sourcetype="Vanguard-Status") OR (sourcetype="Radiant-Status") |rex "Exception taking
snapshot. Entries in snapshot: 0 Error :com.rli.slapd.server.LDAPException:
(?P<IPAddress>\d+\.\d+\.\d+\.\d+)"|rex "ERROR (?P<ConnectionStatus>\w+\s\w+)"|table
_time CurrentTime PrevTime Hostname Status IPAddress ConnectionStatus|eval
CTime=strptime(CurrentTime,"%a %b %d %H:%M:%S %Z %Y")|eval PTime=strptime(PrevTime,"%a
%b %d %H:%M:%S %Z %Y")|eval TimeDiff=(CTime-PTime)|eval
Hostname=if(IPAddress=="192.168.19.11", "openldap.acmefinancial.com", Hostname)|eval
Hostname=if(IPAddress=="192.168.19.10", "ActiveDirectory.acmefinancial.com",
Hostname)|eval Hostname=if(Hostname=="RadiantOne VDS", "RadiantOne
VDS.acmefinancial.com", Hostname)|eval Hostname=if(Hostname=="ActiveDirectory",
"ActiveDirectory.acmefinancial.com", Hostname)|eval
Status=if(ConnectionStatus=="Connection error", "offline", Status)|where
isnotnull(Hostname)|transaction Hostname Status|table _time Hostname Status
```

2.8.10 SSL Forwarding

We took advantage Splunk's built in SSL forwarding capability and configured SSL encryption between forwarders and the indexer. Instructions to enable SSL forwarding can be found at

http://docs.splunk.com/Documentation/Splunk/6.5.3/Security/ConfigureSplunkforwardingtousesignedcertificates.

2.9 TDI ConsoleWorks

ConsoleWorks is a product that provides a portal for remote access to devices, a logging facility with advanced hashing and pattern matching features, and role-based access control for administrators.

2.9.1 How It's Used

ConsoleWorks provides a portal through which privileged users access directory servers and core systems in the lab infrastructure. There are two primary types of access connectors that are configured. The first is a console connector that is either an SSH or Telnet connection to an internal LAN system. The other is a graphical user interface (GUI) connector that can be either through Remote Desktop Protocol (RDP) or Virtual Network Computing (VNC). In this build, SSH was used for the console connections, whereas RDP was used for the GUI connections.

The ConsoleWorks Server sits on a separate subnet that is connected to the Internet via a virtual private network. It is configured to allow connections initiated from the VPN, but it drops connections initiated from the LAN.

Additionally, ConsoleWorks maintains logs of what systems were accessed, the time of access, and by whom. These logs are formatted and prepared for consumption by the Splunk indexer.

2.9.2 Virtual Machine Configuration

ConsoleWorks virtual machine is configured as follows:

- CentOS 7.2.1511
- 1CPU cor
- 8GB of RAM
- 2 NICs
- 100GB of storage.

Network Configuration (LAN)
IPv4 Manual
IPv6 Enabled
IP Address: 192.168.17.11
Netmask: 255.255.255.0
Gateway: 192.168.17.1
DNS Name Servers 192.168.19.10
DNS-Search Domains: acmefinancial.com

Network Configuration (WAN)
IPv4 Manual
IPv6 Enabled

IP Address: 10.33.50.164
Netmask: 255.255.240.0

2.9.3 Firewall Configuration

Enter the following commands in sequence to allow traffic to ports 5176 and 22 ports only. The ConsoleWorks web service listens on port 5176.

1. **firewall-cmd – zone=public – add-port=5176/tcp**
2. **firewall-cmd – zone=public – add-port=22/tcp**

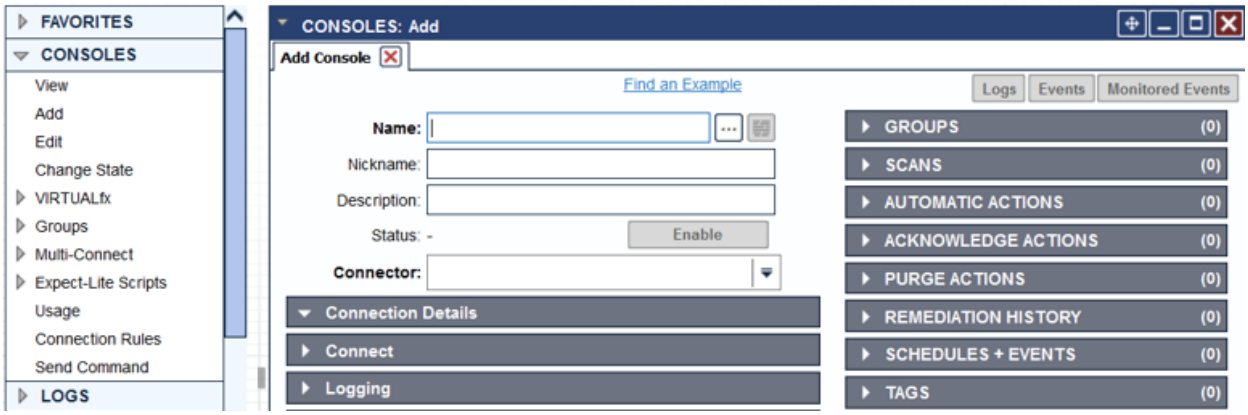
2.9.4 Installation

Installation for Windows, Linux, and Solaris systems can be found at http://support.tditechnologies.com/tags/installation-guides

2.9.5 Console Connection Configuration

To create a console connection:

1. Click on **Consoles>Add.**
2. Type in the name of the Console (for example, **OpenLDAPServer**).
3. Choose the **Connector** type (for example, **SSH on Demand**).
4. Click **Connection Details.** Check the **Exclusive Connect** checkbox.
5. Type in the **Host IP, Port, Username,** and **Password** fields.
6. Click **Save.**



2.9.6 Graphical Gateway Configuration

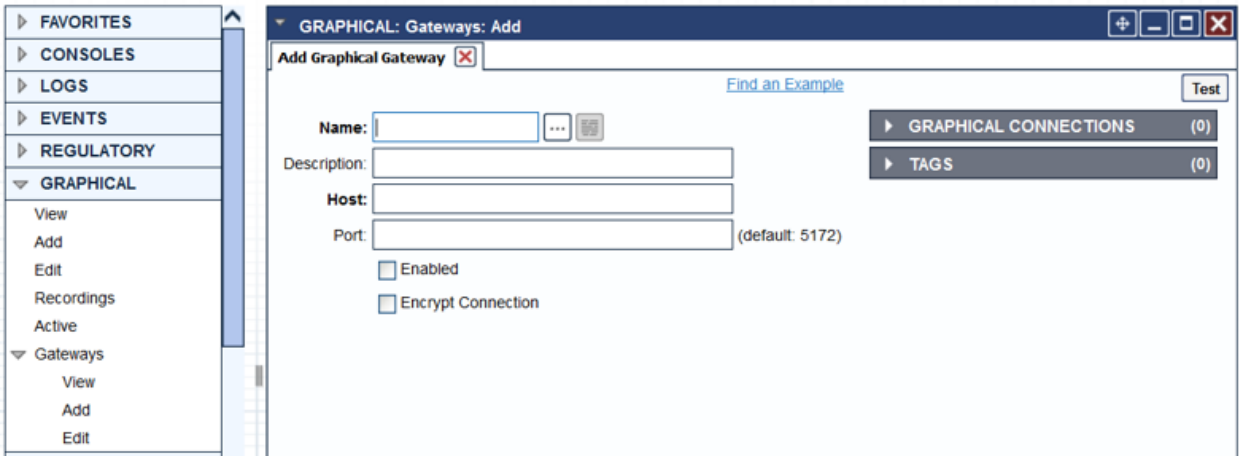
A Graphical Gateway is required to make an RDP or VNC connection to a server.

To configure a Graphical Gateway, you need to obtain and install the graphical gateway package from TDi Technologies Inc. The following steps describe installing and starting the service once the package is obtained.

```
rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-version>.rpm
/opt/gui_gateway/install_local.sh
/opt/ConsoleWorks/bin/cw_start <invocation name> (created during installation)
service gui_gatewayd start
```

Install the Graphical gateway:

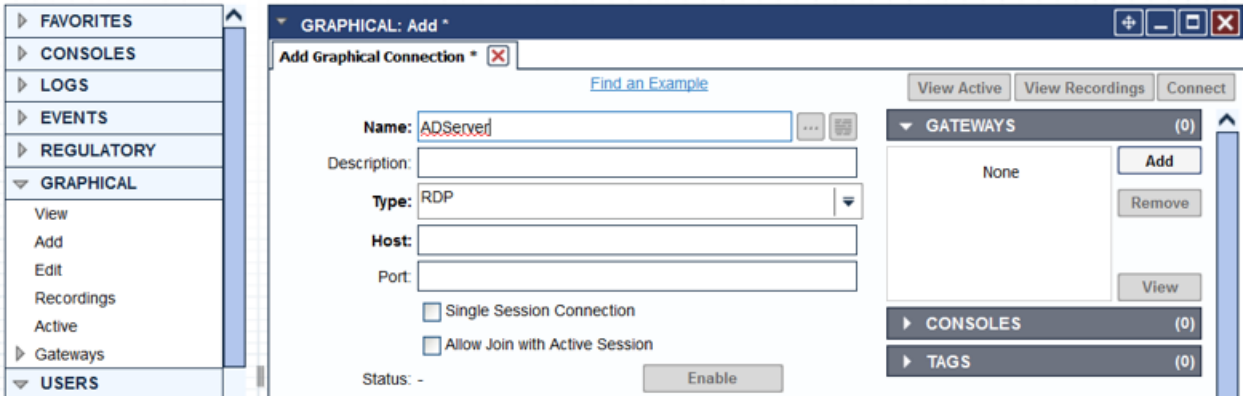
1. On the landing page on your ConsoleWorks server, click **GRAPHICAL>Gateways>Add**.
2. Give it a name, then set **Host** as Localhost and **Port** as 5172.
3. Check **Enabled** checkbox and click **Save**.
4. Verify it works by clicking **Test** in the top-left corner.



2.9.7 Graphical Connection Configuration

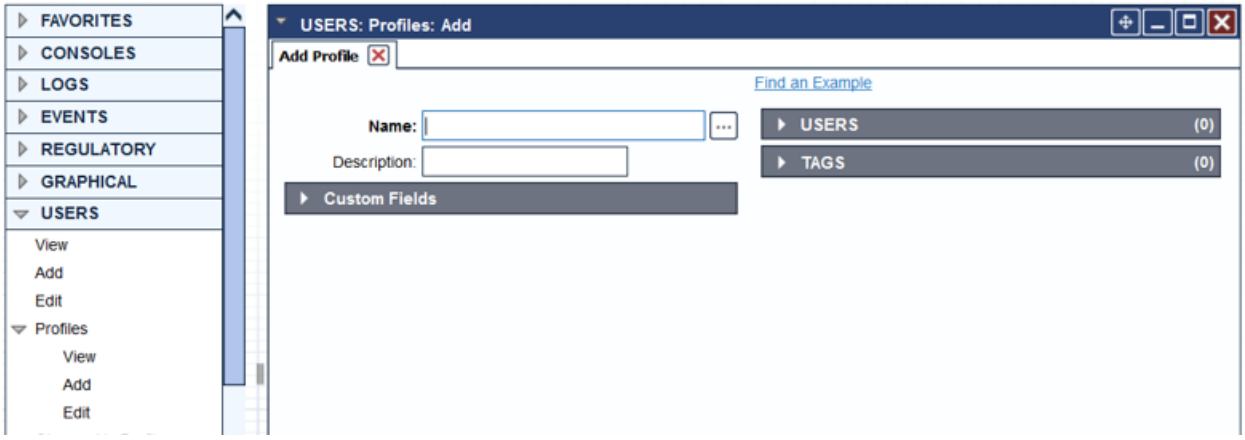
Configure the Graphical gateway:

1. On the landing page of your ConsoleWorks server, click **GRAPHICAL>Add.**
2. Type in the name of the Graphical connection (for example, **ADServer**).
3. Choose a protocol in the **Type** drop-down list (for example, **RDP**).
4. Enter the name or IP address of the server in the **Host** field.
5. Type in the port number in the **Port** field. Enter **3389** for RDP.
6. Click **Save.**



2.9.8 Profile Creation

1. Click **USERS>Profiles>Add.**
2. Type in the name of the profile in the **Name** field.
3. Click **Save.**

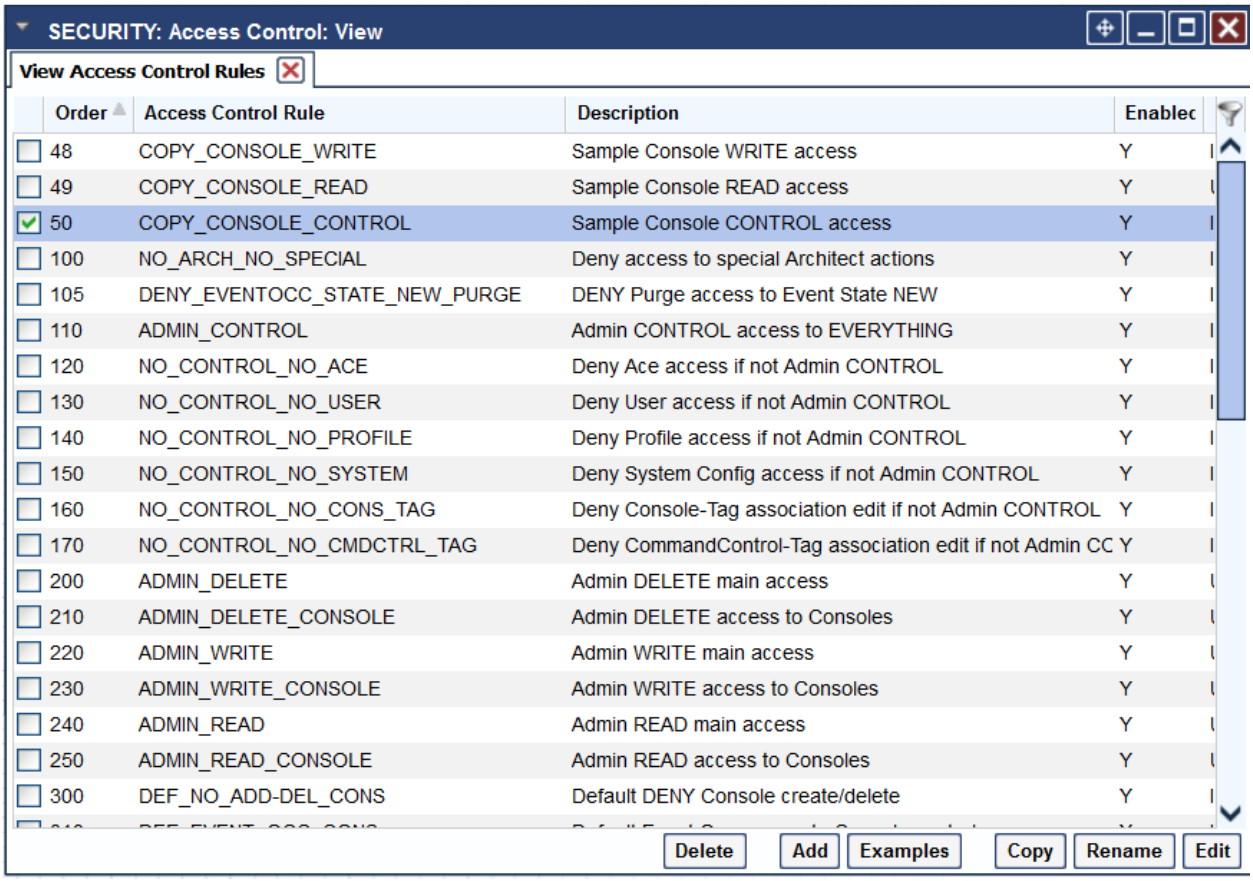


2.9.9 Access Controls

Access controls are rules that determine the level of access a user has to a Console or Graphical connection. These rules can be associated with profiles and tags, which in turn can be associated with a user to determine what a user has access to when logged in. In our build, we grouped privileged users based on the servers they needed access to, created profiles that mirrored these groups, linked the users to these profiles, and associated the access rules to the profiles.

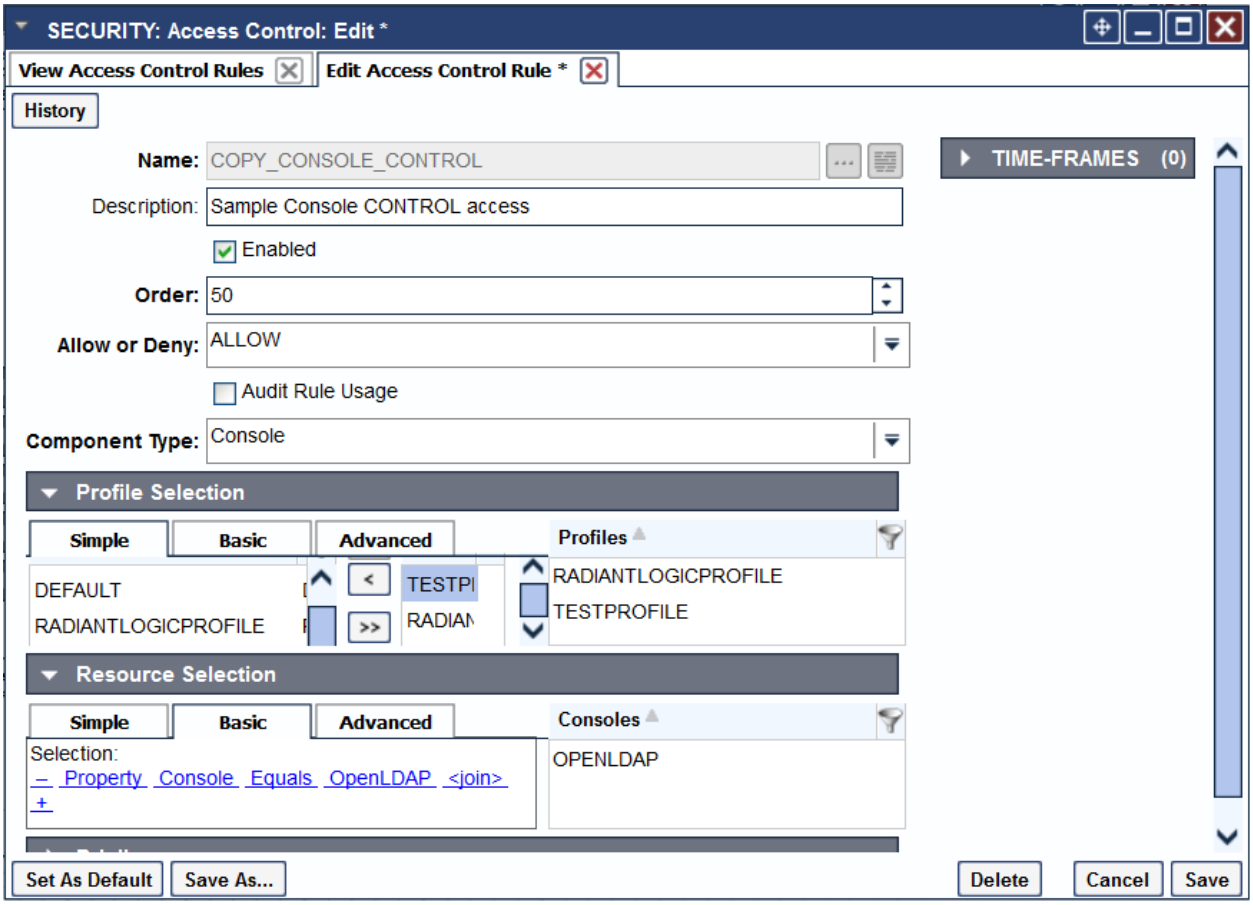
Create new access control rules:

1. Copy the **CONSOLE_CONTROL** access control rule and assign it a number below 100. Access control rules with lower numbers have priority over higher numbers.
2. Select the newly copied access rule and click Edit.



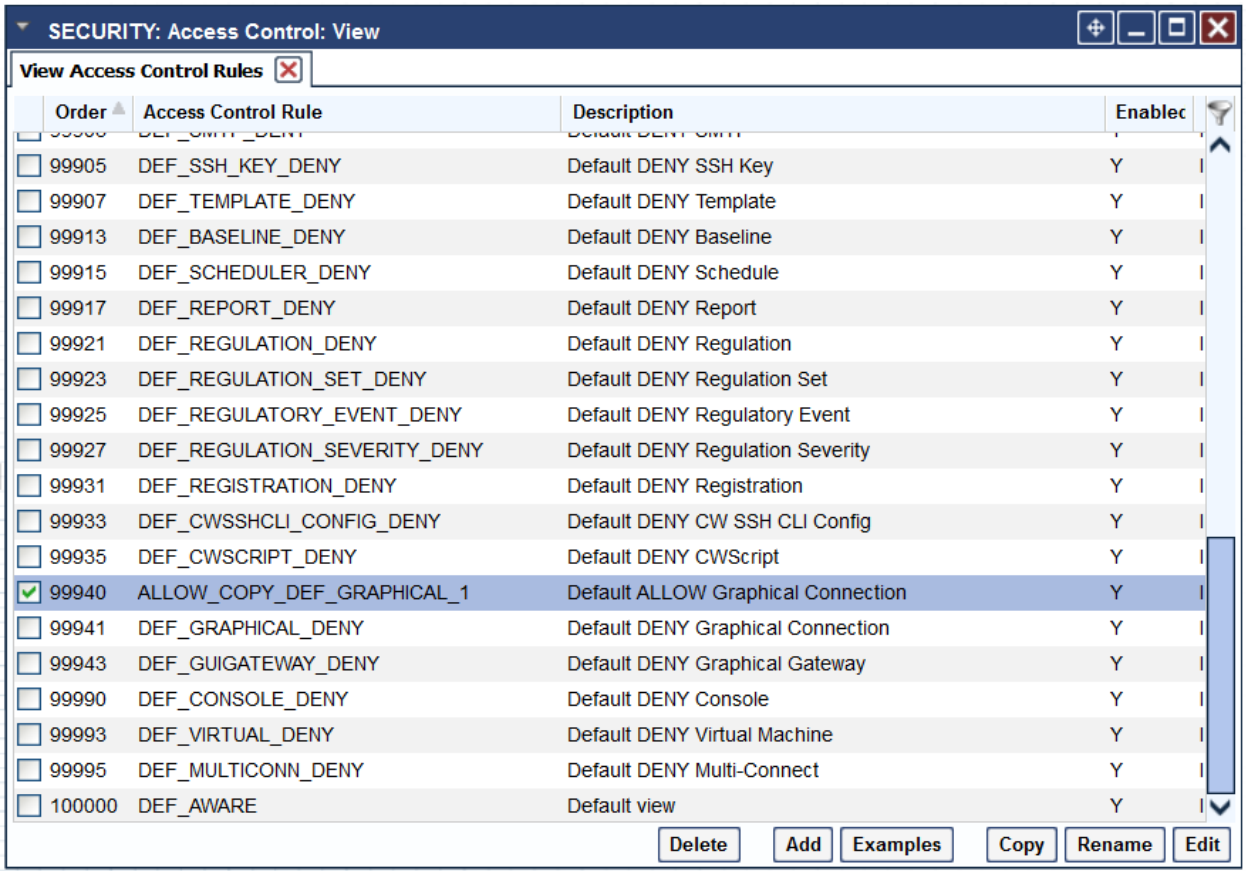
To create a profile:

1. In the **Allow or Deny** field, Select **ALLOW**.
2. In the component **Type**, select **Console.**
3. In the **Profile Selection** area, select the profile of choice from the **Simple** tab and click the double arrows. Make sure it appears in the **Profiles** section.
4. In the **Resource Selection** section, select the Console you want users associated with this profile to connect to. Select the **OpenLDAP** console.

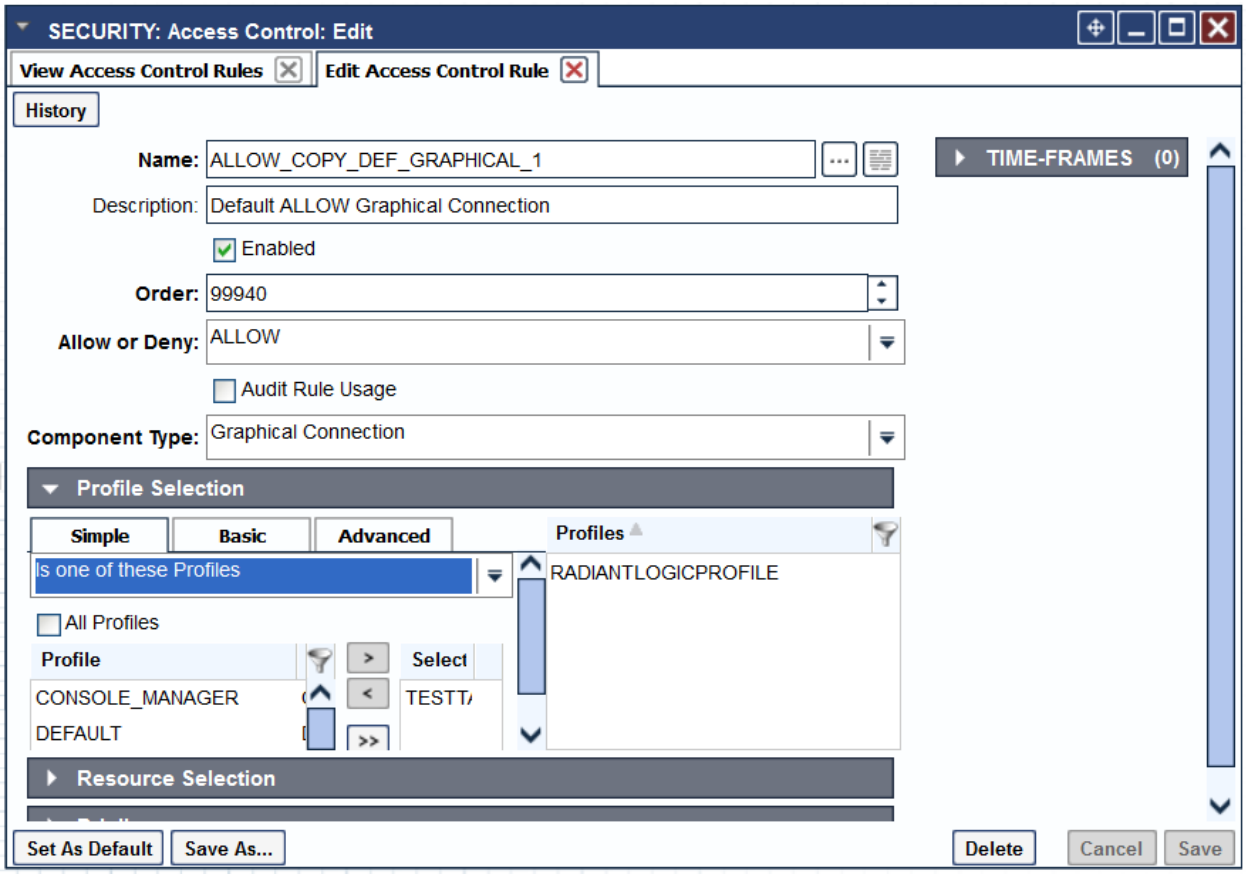


2357

2358 1. To set access control rules for Graphical connections: Copy the **DEF_GRAPHICAL_DENY** and
2359 rename as **ALLOW_COPY_DEF_GRAPHICAL_1**.
2360 2. Click **Edit.**

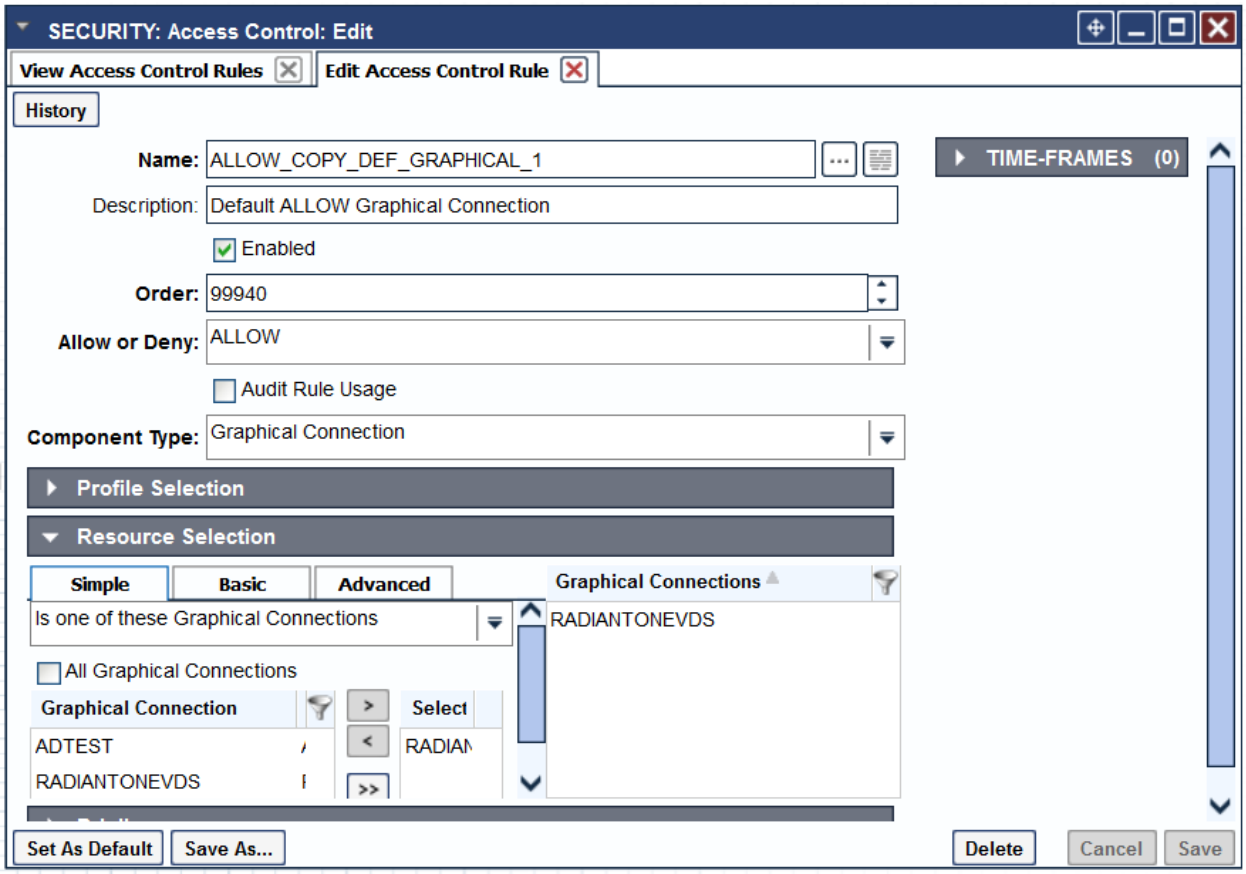


1. To link an access control rule to a profile and a resource, first follow these steps:Edit this rule and change the **Allow or Deny** field from DENY to **ALLOW.**
2. Change the Description to **Default ALLOW Graphical Connection.**
3. Ensure that the order number is lower than the Default DENY Graphical Connection rule (DEF_GRAPHICAL_DENY).
4. Under Profile Selection, click the **Simple** tab and select “Is one of these Profiles.”
5. Select the profile of choice and make sure it appears on the right under Profiles.



2369

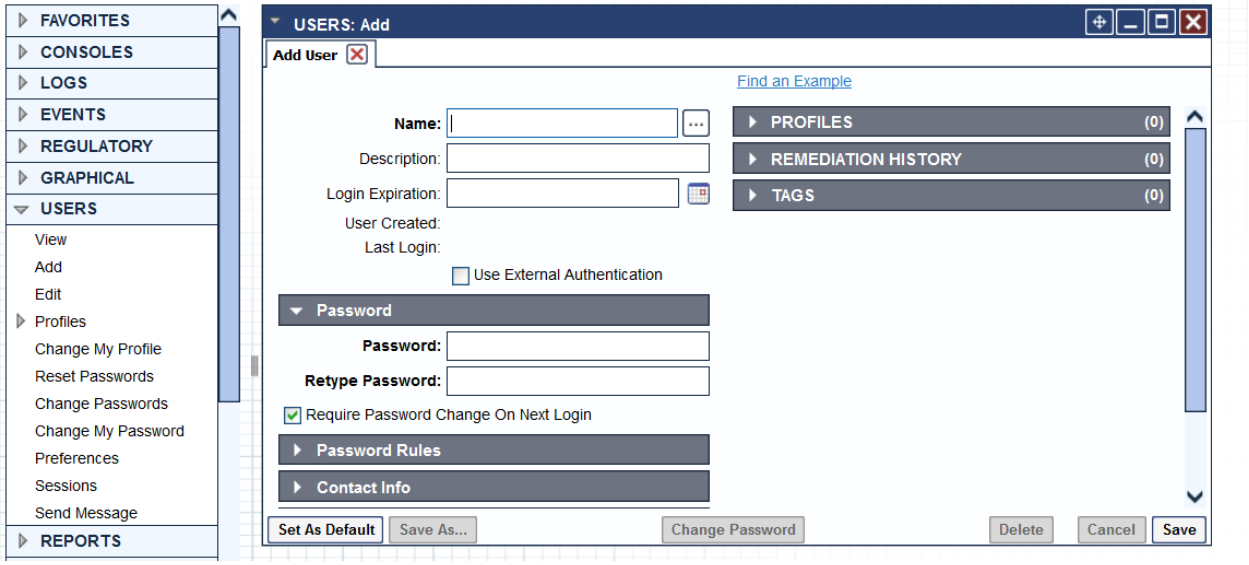
2370 1. Next, you will need to **Select** the Graphical Connection of choice such as RADIANTONE VDS.
2371 2. Click the double arrow and ensure that it appears on the right.



2372

2373 To add users and link to a profile:

2374 1. Click on **USERS > Add.**
2375 2. Type in the username in **Name** field.
2376 3. Enter the password in the **Password** and **Retype Password** fields.
2377 4. Click on **PROFILES > Add.**
2378 5. Select the profile of choice.



2.9.10 User Auditing

An audit trail of ConsoleWorks user activity is captured in a file and forwarded to Splunk for further analysis. The the information includes username, logon timestamp, and the target server to which the user is connecting. The connection reporting script below parses the ConsoleWorks logs and writes the output to a file. The bash connectionreporting script removes duplicate lines. The bashconenctionreporting script is scheduled using cron to run every minute using the following /etc/crontab configuration.

2.9.11 Cron Configuration: /etc/crontab

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
# For details see man 4 crontabs
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
 *  *  *  *  * root      /etc/cron.daily/bashconnectionreporting
```

2.9.12 Scripts: connectionreporting

```
#!/usr/bin/python3.5
#Script identifies ConsoleWorks users, connection times and their targets
```

```
#import the OS module
import os
#Store the ConsoleWorks log directory in the "directory" variable
directory = "/opt/ConsoleWorks/FSARM/log"
#Change directory to the Log dir
os.chdir(directory)
#Iterate through files in log dir and look for strings shown in the
#IF statements. Matching lines are written to file
for file in os.listdir(directory):
   with open(file, 'r') as file_object:
      for line in file_object:
         if "CONWRKS Audit:: User:" in line:
            with open('/var/log/connections.out','a') as outfile_object:
               outfile_object.write(line)
         if "connecting" in line:
            with open('/var/log/connections.out','a') as outfile_object:
               outfile_object.write(line)
         if "disconnecting" in line:
            with open('/var/log/connections.out','a') as outfile_object:
               outfile_object.write(line)
```

2.9.13 Scripts: bashconnectionreporting

```
#!/bin/bash
#Calls python script that reads ConsoleWorks log files and outputs to
#/var/log/connections.out
/etc/cron.daily/connectionreporting
#This line removes duplicate lines from the connections.out file and outputs them
# to connections.log
awk '!seen[$0]++' /var/log/connections.out > /var/log/connections.log
```

2.10 Network Firewall Configuration

pfSense virtual devices were used as firewall routers for each subnet and were configured to restrict traffic as appropriate. The subnets listed below have critical services and resources that need to be accessed from devices external to the LAN. We have made the exact configuration used in each pfSense firewall available in XML format. This can be imported directly into another pfSense device. It is important to note that an IPSEC VPN connection was made to the offsite RACF LDAP directory server. The IPSEC VPN configuration was set up in the firewall for the backbone subnet.

2.10.1 Firewall Configuration for Backbone Subnet

```
<?xml version="1.0"?>
<pfsense>
	<version>15.4</version>
	<lastchange/>
	<theme>pfsense_ng</theme>
	<system>
		<optimization>normal</optimization>
		<hostname>pfsenseVLAN13</hostname>
		<domain>acmefinancial.com</domain>
		<group>
			<name>all</name>
			<description><![CDATA[All Users]]></description>
			<scope>system</scope>
			<gid>1998</gid>
			<member>0</member>
		</group>
		<group>
			<name>admins</name>
			<description><![CDATA[System Administrators]]></description>
			<scope>system</scope>
			<gid>1999</gid>
			<member>0</member>
			<priv>page-all</priv>
		</group>
		<user>
			<name>admin</name>
			<descr><![CDATA[System Administrator]]></descr>
			<scope>system</scope>
			<groupname>admins</groupname>
			<password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
			<uid>0</uid>
			<priv>user-shell-access</priv>
		</user>
```

```
<nextuid>2000</nextuid>
<nextgid>2000</nextgid>
<timezone>America/New_York</timezone>
<time-update-interval/>
<timeservers>10.97.74.8</timeservers>
<webgui>
	<protocol>http</protocol>
	<loginautocomplete/>
	<ssl-certref>5720a0502b277</ssl-certref>
	<dashboardcolumns>2</dashboardcolumns>
	<webguicss>pfsense.css</webguicss>
</webgui>
<disablesegmentationoffloading/>
<disablelargereceiveoffloading/>
<ipv6allow/>
<powerd_ac_mode>hadp</powerd_ac_mode>
<powerd_battery_mode>hadp</powerd_battery_mode>
<powerd_normal_mode>hadp</powerd_normal_mode>
<bogons>
	<interval>monthly</interval>
</bogons>
<language>en_US</language>
<dns1gw>GW_WAN</dns1gw>
<dns2gw>GW_WAN</dns2gw>
<dns3gw>none</dns3gw>
<dns4gw>none</dns4gw>
<maximumstates/>
<aliasesresolveinterval/>
<maximumtableentries/>
<maximumfrags/>
<enablenatreflectionpurenat>yes</enablenatreflectionpurenat>
<enablebinatreflection>yes</enablebinatreflection>
<enablenatreflectionhelper>yes</enablenatreflectionhelper>
<reflectiontimeout/>
```

```
2507                <dnsserver>10.97.74.8</dnsserver>
2508                <dnsserver>10.63.255.2</dnsserver>
2509          </system>
2510          <interfaces>
2511                <wan>
2512                      <if>em0</if>
2513                      <descr><![CDATA[WAN]]></descr>
2514                      <enable/>
2515                      <spoofmac/>
2516                      <ipaddr>10.33.50.34</ipaddr>
2517                      <subnet>28</subnet>
2518                      <gateway>GW_WAN</gateway>
2519                      <ipaddrv6/>
2520                      <subnetv6/>
2521                      <gatewayv6/>
2522                </wan>
2523                <lan>
2524                      <enable/>
2525                      <if>em1</if>
2526                      <ipaddr>192.168.13.1</ipaddr>
2527                      <subnet>24</subnet>
2528                      <ipaddrv6/>
2529                      <subnetv6/>
2530                      <media/>
2531                      <mediaopt/>
2532                      <track6-interface>wan</track6-interface>
2533                      <track6-prefix-id>0</track6-prefix-id>
2534                      <gateway/>
2535                      <gatewayv6/>
2536                </lan>
2537          </interfaces>
2538          <staticroutes>
2539                <route>
2540                      <network>192.168.14.0/24</network>
```

```
                <gateway>VLAN2014</gateway>
                <descr/>
        </route>
        <route>
                <network>192.168.19.0/24</network>
                <gateway>VLAN2019</gateway>
                <descr/>
        </route>
        <route>
                <network>192.168.18.0/24</network>
                <gateway>VLAN2018</gateway>
                <descr/>
        </route>
        <route>
                <network>192.168.15.0/24</network>
                <gateway>VLAN2015</gateway>
                <descr/>
        </route>
        <route>
                <network>192.168.16.0/24</network>
                <gateway>VLAN2016</gateway>
                <descr/>
        </route>
        <route>
                <network>192.168.17.0/24</network>
                <gateway>VLAN2017</gateway>
                <descr/>
        </route>
        <route>
                <network>192.168.20.0/24</network>
                <gateway>VLAN2020</gateway>
                <descr/>
        </route>
        <route>
```

```
                    <network>10.33.50.160/28</network>
                    <gateway>VLAN2066</gateway>
                    <descr><![CDATA[Route to Vendor Net]]></descr>
              </route>
        </staticroutes>
        <dhcpd>
              <lan>
                    <enable/>
                    <range>
                          <from>192.168.13.100</from>
                          <to>192.168.13.150</to>
                    </range>
                    <failover_peerip/>
                    <dhcpleaseinlocaltime/>
                    <defaultleasetime/>
                    <maxleasetime/>
                    <netmask/>
                    <dnsserver>192.168.19.10</dnsserver>
                    <gateway/>
                    <domain>acmefinancial.com</domain>
                    <domainsearchlist>acmefinancial.com</domainsearchlist>
                    <ddnsdomain/>
                    <ddnsdomainprimary/>
                    <ddnsdomainkeyname/>
                    <ddnsdomainkey/>
                    <mac_allow/>
                    <mac_deny/>
                    <tftp/>
                    <ldap/>
                    <nextserver/>
                    <filename/>
                    <filename32/>
                    <filename64/>
                    <rootpath/>
```

```
                <numberoptions/>
            </lan>
            <opt1>
                <enable/>
                <range>
                    <from>192.168.14.100</from>
                    <to>192.168.14.150</to>
                </range>
                <dhcpleaseinlocaltime/>
            </opt1>
            <opt2>
                <enable/>
                <range>
                    <from>192.168.15.100</from>
                    <to>192.168.15.150</to>
                </range>
                <dhcpleaseinlocaltime/>
            </opt2>
            <opt3>
                <enable/>
                <range>
                    <from>192.168.16.100</from>
                    <to>192.168.16.150</to>
                </range>
                <dhcpleaseinlocaltime/>
            </opt3>
        </dhcpd>
        <snmpd>
            <syslocation/>
            <syscontact/>
            <rocommunity>public</rocommunity>
        </snmpd>
        <diag>
            <ipv6nat>
```

```
                <ipaddr/>
            </ipv6nat>
        </diag>
        <bridge/>
        <syslog/>
        <nat>
            <outbound>
                <mode>automatic</mode>
            </outbound>
            <onetoone>
                <external>10.33.50.44</external>
                <descr><![CDATA[mapping to 2020 pfsense firewall ]]></descr>
                <interface>wan</interface>
                <source>
                    <address>192.168.13.20</address>
                </source>
                <destination>
                    <any/>
                </destination>
            </onetoone>
            <onetoone>
                <external>10.33.50.42</external>
                <descr><![CDATA[Mapping to Pfsense firewall]]></descr>
                <interface>wan</interface>
                <source>
                    <address>192.168.13.17</address>
                </source>
                <destination>
                    <any/>
                </destination>
            </onetoone>
            <onetoone>
                <external>10.33.50.35</external>
                <descr><![CDATA[Mapping to Splunk]]></descr>
```

```
                        <interface>wan</interface>
                        <source>
                                <address>192.168.17.11</address>
                        </source>
                        <destination>
                                <any/>
                        </destination>
                </onetoone>
                <onetoone>
                        <external>10.33.50.41</external>
                        <descr><![CDATA[Mapping to Pfsense firewall]]></descr>
                        <interface>wan</interface>
                        <source>
                                <address>192.168.19.11</address>
                        </source>
                        <destination>
                                <any/>
                        </destination>
                </onetoone>
                <onetoone>
                        <external>10.33.50.36</external>
                        <descr><![CDATA[Mapping to Hytrust ESXi Server]]></descr>
                        <interface>wan</interface>
                        <source>
                                <address>192.168.20.12</address>
                        </source>
                        <destination>
                                <any/>
                        </destination>
                </onetoone>
                <onetoone>
                        <external>10.33.50.37</external>
                        <descr><![CDATA[NAT Mapping to RadiantOne VDS]]></descr>
                        <interface>wan</interface>
```

```
                        <source>
                              <address>192.168.14.11</address>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                  </onetoone>
                  <onetoone>
                        <external>10.33.50.38</external>
                        <descr><![CDATA[NAT Mapping to Hytrust CloudControl VM]]></descr>
                        <interface>wan</interface>
                        <source>
                              <address>192.168.20.11</address>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                  </onetoone>
                  <onetoone>
                        <external>10.33.50.40</external>
                        <descr><![CDATA[Mapping to ActiveDirectory]]></descr>
                        <interface>wan</interface>
                        <source>
                              <address>192.168.19.10</address>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                  </onetoone>
                  <onetoone>
                        <external>10.33.50.43</external>
                        <descr><![CDATA[VIP for ConsoleWorks -- Mapping to Internal
Address]]></descr>
                        <interface>wan</interface>
```

```
                        <source>
                              <address>192.168.17.11</address>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                  </onetoone>
                  <onetoone>
                        <external>10.33.50.45</external>
                        <descr><![CDATA[VIP for CentOSToAD-- Mapping to Internal
Address]]></descr>
                        <interface>wan</interface>
                        <source>
                              <address>192.168.19.30</address>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                  </onetoone>
                  <onetoone>
                        <external>10.33.50.46</external>
                        <descr><![CDATA[AlertEnterprise Enterprise Guardian]]></descr>
                        <interface>wan</interface>
                        <source>
                              <address>192.168.17.114</address>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                  </onetoone>
                  <rule>
                        <source>
                              <any/>
                        </source>
```

```
                        <destination>
                                <network>wanip</network>
                                <port>1322</port>
                        </destination>
                        <protocol>tcp</protocol>
                        <target>192.168.13.130</target>
                        <local-port>80</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Mapping to pfsense 192.168.13.130]]></descr>
                        <associated-rule-id>nat_581795efbc2944.51341500</associated-rule-
id>
                        <created>
                                <time>1477940719</time>
                                <username>admin@192.168.13.139</username>
                        </created>
                        <updated>
                                <time>1477940861</time>
                                <username>admin@192.168.13.139</username>
                        </updated>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <address>10.33.50.41</address>
                                <port>80</port>
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.19.11</target>
                        <local-port>80</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port forward to openldap; Add /phpldapadmin to
address]]></descr>
```

```
                        <associated-rule-id>nat_57bf0c96d083f4.07194849</associated-rule-
id>
                        <created>
                                <time>1472138390</time>
                                <username>admin@10.97.67.137</username>
                        </created>
                        <updated>
                                <time>1473431620</time>
                                <username>admin@10.97.67.134</username>
                        </updated>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <address>10.33.50.41</address>
                                <port>22</port>
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.19.11</target>
                        <local-port>22</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port forward to openldap; ]]></descr>
                        <associated-rule-id>nat_57f555406f2de3.01889708</associated-rule-
id>
                        <created>
                                <time>1475695936</time>
                                <username>admin@10.97.67.145</username>
                        </created>
                        <updated>
                                <time>1475695966</time>
                                <username>admin@10.97.67.145</username>
                        </updated>
                </rule>
```

```
2848                <rule>
2849                      <source>
2850                            <any/>
2851                      </source>
2852                      <destination>
2853                            <address>10.33.50.35</address>
2854                            <port>8000</port>
2855                      </destination>
2856                      <protocol>tcp/udp</protocol>
2857                      <target>192.168.17.10</target>
2858                      <local-port>8000</local-port>
2859                      <interface>wan</interface>
2860                      <descr><![CDATA[Splunk port 8000 Web Interface]]></descr>
2861                      <associated-rule-id>nat_57d825ba865df6.65796295</associated-rule-
2862 id>
2863                      <created>
2864                            <time>1473783226</time>
2865                            <username>admin@10.97.67.152</username>
2866                      </created>
2867                      <updated>
2868                            <time>1473785552</time>
2869                            <username>admin@10.97.67.152</username>
2870                      </updated>
2871                </rule>
2872                <rule>
2873                      <source>
2874                            <any/>
2875                      </source>
2876                      <destination>
2877                            <address>10.33.50.35</address>
2878                            <port>22</port>
2879                      </destination>
2880                      <protocol>tcp/udp</protocol>
2881                      <target>192.168.17.10</target>
```

```
                        <local-port>22</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Splunk SSH ]]></descr>
                        <associated-rule-id>nat_582ef78ed63d23.63868026</associated-rule-
id>
                        <updated>
                              <time>1479473038</time>
                              <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                              <time>1479473038</time>
                              <username>admin@10.97.67.135</username>
                        </created>
                  </rule>
                  <rule>
                        <source>
                              <any/>
                        </source>
                        <destination>
                              <address>10.33.50.42</address>
                              <port>1314</port>
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.13.14</target>
                        <local-port>80</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port Forward to 192.168.13.14 Pf]]></descr>
                        <associated-rule-id>nat_57c01545c247f0.43308393</associated-rule-
id>
                        <updated>
                              <time>1472206149</time>
                              <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                              <time>1472206149</time>
```

```
                        <username>admin@10.97.67.135</username>
                    </created>
                </rule>
                <rule>
                    <source>
                        <any/>
                    </source>
                    <destination>
                        <address>10.33.50.42</address>
                        <port>1315</port>
                    </destination>
                    <protocol>tcp/udp</protocol>
                    <target>192.168.13.15</target>
                    <local-port>80</local-port>
                    <interface>wan</interface>
                    <descr><![CDATA[Port Forward to 192.168.13.15 Pf]]></descr>
                    <associated-rule-id>nat_57c0163d6e2de9.62906352</associated-rule-
id>
                    <updated>
                        <time>1472206397</time>
                        <username>admin@10.97.67.135</username>
                    </updated>
                    <created>
                        <time>1472206397</time>
                        <username>admin@10.97.67.135</username>
                    </created>
                </rule>
                <rule>
                    <source>
                        <any/>
                    </source>
                    <destination>
                        <address>10.33.50.42</address>
                        <port>1316</port>
```

```
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.13.16</target>
                        <local-port>80</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port Forward to 192.168.13.16 Pf]]></descr>
                        <associated-rule-id>nat_57c01682da98c4.72334719</associated-rule-
id>
                        <updated>
                              <time>1472206466</time>
                              <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                              <time>1472206466</time>
                              <username>admin@10.97.67.135</username>
                        </created>
                  </rule>
                  <rule>
                        <source>
                              <any/>
                        </source>
                        <destination>
                              <address>10.33.50.42</address>
                              <port>1317</port>
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.13.17</target>
                        <local-port>80</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port Forward to 192.168.13.17 Pf]]></descr>
                        <associated-rule-id>nat_57c01787b4e891.75909166</associated-rule-
id>
                        <updated>
                              <time>1472206727</time>
                              <username>admin@10.97.67.135</username>
```

```
                        </updated>
                        <created>
                                <time>1472206727</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <address>10.33.50.42</address>
                                <port>1318</port>
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.13.18</target>
                        <local-port>80</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port Forward to 192.168.13.18 Pf]]></descr>
                        <associated-rule-id>nat_57c017be3dffa1.16882401</associated-rule-
id>
                        <updated>
                                <time>1472206782</time>
                                <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                                <time>1472206782</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
```

```
                        <destination>
                                <address>10.33.50.42</address>
                                <port>1319</port>
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.13.19</target>
                        <local-port>80</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port Forward to 192.168.13.19 Pf]]></descr>
                        <associated-rule-id>nat_57c017e1e48d65.86612217</associated-rule-
id>
                        <updated>
                                <time>1472206817</time>
                                <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                                <time>1472206817</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <address>10.33.50.42</address>
                                <port>1320</port>
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.13.20</target>
                        <local-port>80</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port Forward to 192.168.13.20 Pf]]></descr>
                        <associated-rule-id>nat_57c0187fd4a074.12397754</associated-rule-
id>
```

```
                        <created>
                                <time>1472206975</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                        <updated>
                                <time>1477940348</time>
                                <username>admin@192.168.13.139</username>
                        </updated>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <address>10.33.50.42</address>
                                <port>2006</port>
                        </destination>
                        <protocol>tcp/udp</protocol>
                        <target>192.168.20.6</target>
                        <local-port>443</local-port>
                        <interface>wan</interface>
                        <descr><![CDATA[Port Forward to Hytrust Cloud Control
192.168.20.6]]></descr>
                        <associated-rule-id>nat_585ab274d8bce0.68941358</associated-rule-
id>
                        <updated>
                                <time>1482338932</time>
                                <username>admin@10.97.67.139</username>
                        </updated>
                        <created>
                                <time>1482338932</time>
                                <username>admin@10.97.67.139</username>
                        </created>
                </rule>
                <separator/>
```

```
        </nat>
        <filter>
                <rule>
                        <id/>
                        <tracker>1483547179</tracker>
                        <type>pass</type>
                        <interface>enc0</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <any/>
                        </destination>
                        <descr><![CDATA[Allow IPSEC Traffic in both directions to
pass]]></descr>
                        <updated>
                                <time>1483547179</time>
                                <username>admin@10.97.67.165</username>
                        </updated>
                        <created>
                                <time>1483547179</time>
```

```
                        <username>admin@10.97.67.165</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1481038469</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <source>
                        <address>192.168.14.111</address>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr><![CDATA[Allow Radiant (192.168.14.111) to go anywhere -
LAN]]></descr>
                <updated>
                        <time>1481038469</time>
                        <username>admin@10.97.67.155</username>
                </updated>
                <created>
```

```
                        <time>1481038469</time>
                        <username>admin@10.97.67.155</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1481134883</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <source>
                        <address>192.168.13.135</address>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr><![CDATA[Allow CA.acmefinancial to go anywhere]]></descr>
                <updated>
                        <time>1481134883</time>
                        <username>admin@10.97.67.146</username>
                </updated>
                <created>
```

```
                        <time>1481134883</time>
                        <username>admin@10.97.67.146</username>
                    </created>
                </rule>
                <rule>
                    <id/>
                    <tracker>1481038517</tracker>
                    <type>pass</type>
                    <interface>lan</interface>
                    <ipprotocol>inet</ipprotocol>
                    <tag/>
                    <tagged/>
                    <direction>any</direction>
                    <quick>yes</quick>
                    <floating>yes</floating>
                    <max/>
                    <max-src-nodes/>
                    <max-src-conn/>
                    <max-src-states/>
                    <statetimeout/>
                    <statetype>keep state</statetype>
                    <os/>
                    <source>
                        <address>192.168.17.100</address>
                    </source>
                    <destination>
                        <any/>
                    </destination>
                    <descr><![CDATA[Allow Radiant (192.168.17.100) to go anywhere -
LAN]]></descr>
                    <updated>
                        <time>1481038517</time>
                        <username>admin@10.97.67.155</username>
                    </updated>
```

```
                        <created>
                                <time>1481038517</time>
                                <username>admin@10.97.67.155</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1478010422</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <any/>
                        </destination>
                        <descr/>
                        <updated>
                                <time>1478010422</time>
                                <username>admin@10.97.66.18</username>
                        </updated>
```

```
                <created>
                        <time>1478010422</time>
                        <username>admin@10.97.66.18</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1480540664</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr><![CDATA[Allow all LAN traffic to go to anywhere]]></descr>
                <updated>
                        <time>1480540664</time>
                        <username>admin@10.97.67.140</username>
                </updated>
```

```
                        <created>
                                <time>1480540664</time>
                                <username>admin@10.97.67.140</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1472208251</tracker>
                        <type>pass</type>
                        <interface>lan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp/udp</protocol>
                        <source>
                                <address>192.168.0.0/16</address>
                        </source>
                        <destination>
                                <address>192.168.0.0/16</address>
                        </destination>
                        <descr><![CDATA[Allow traffic going from local subnet to local
subne]]></descr>
                        <updated>
                                <time>1472208251</time>
```

```
                        <username>admin@10.97.67.135</username>
                </updated>
                <created>
                        <time>1472208251</time>
                        <username>admin@10.97.67.135</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1472216936</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <address>192.168.0.0/16</address>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr><![CDATA[Allow traffic going from local subnet to
anywhere]]></descr>
```

```
                        <updated>
                                <time>1472216936</time>
                                <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                                <time>1472216936</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1476720725</tracker>
                        <type>pass</type>
                        <interface>enc0</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <any/>
                        </destination>
```

```
                    <descr><![CDATA[Allow  All traffic sourced from Tunnel to Anywhere
o]]></descr>
                    <updated>
                          <time>1476720725</time>
                          <username>admin@10.97.67.137</username>
                    </updated>
                    <created>
                          <time>1476720725</time>
                          <username>admin@10.97.67.137</username>
                    </created>
             </rule>
             <rule>
                    <id/>
                    <tracker>1471551236</tracker>
                    <type>pass</type>
                    <interface>wan</interface>
                    <ipprotocol>inet</ipprotocol>
                    <tag/>
                    <tagged/>
                    <max/>
                    <max-src-nodes/>
                    <max-src-conn/>
                    <max-src-states/>
                    <statetimeout/>
                    <statetype>keep state</statetype>
                    <os/>
                    <protocol>tcp/udp</protocol>
                    <source>
                          <any/>
                    </source>
                    <destination>
                          <any/>
                    </destination>
                    <descr><![CDATA[Allow all TCP/UDP Traffic sourced from WAN
interface]]></descr>
```

```
                        <updated>
                                <time>1471551236</time>
                                <username>admin@10.97.67.136</username>
                        </updated>
                        <created>
                                <time>1471551236</time>
                                <username>admin@10.97.67.136</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1470759134</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp/udp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <network>(self)</network>
                        </destination>
                        <descr><![CDATA[Rule to allow connection to firewall -can be
tighten]]></descr>
                        <updated>
```

```
                        <time>1470759134</time>
                        <username>admin@192.168.13.135</username>
                </updated>
                <created>
                        <time>1470759134</time>
                        <username>admin@192.168.13.135</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1461788221</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr/>
                <updated>
                        <time>1461788221</time>
                        <username>admin@192.168.1.2</username>
```

```
                        </updated>
                        <created>
                                <time>1461788221</time>
                                <username>admin@192.168.1.2</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1465934823</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>icmp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <any/>
                        </destination>
                        <descr><![CDATA[Easy Rule: Passed from Firewall Log
View]]></descr>
                        <created>
                                <time>1465934786</time>
                                <username>Easy Rule</username>
                        </created>
```

```
                        <updated>
                                <time>1465934839</time>
                                <username>admin@192.168.13.101</username>
                        </updated>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                                <address>192.168.19.11</address>
                                <port>80</port>
                        </destination>
                        <descr><![CDATA[NAT Port forward to openldap; Add /phpldapadmin to
address]]></descr>
                        <associated-rule-id>nat_57bf0c96d083f4.07194849</associated-rule-
id>
                        <tracker>1472138390</tracker>
                        <created>
                                <time>1472138390</time>
                                <username>NAT Port Forward</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                                <address>192.168.13.14</address>
                                <port>80</port>
                        </destination>
```

```
                        <descr><![CDATA[NAT Port Forward to 192.168.13.14 Pf]]></descr>
                        <associated-rule-id>nat_57c01545c247f0.43308393</associated-rule-
id>
                        <tracker>1472206149</tracker>
                        <created>
                                <time>1472206149</time>
                                <username>NAT Port Forward</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                                <address>192.168.13.15</address>
                                <port>80</port>
                        </destination>
                        <descr><![CDATA[NAT Port Forward to 192.168.13.15 Pf]]></descr>
                        <associated-rule-id>nat_57c0163d6e2de9.62906352</associated-rule-
id>
                        <tracker>1472206397</tracker>
                        <created>
                                <time>1472206397</time>
                                <username>NAT Port Forward</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
```

```
                        <address>192.168.13.16</address>
                        <port>80</port>
                    </destination>
                    <descr><![CDATA[NAT Port Forward to 192.168.13.16 Pf]]></descr>
                    <associated-rule-id>nat_57c01682da98c4.72334719</associated-rule-
id>
                    <tracker>1472206466</tracker>
                    <created>
                        <time>1472206466</time>
                        <username>NAT Port Forward</username>
                    </created>
                </rule>
                <rule>
                    <source>
                        <any/>
                    </source>
                    <interface>wan</interface>
                    <protocol>tcp/udp</protocol>
                    <destination>
                        <address>192.168.13.17</address>
                        <port>80</port>
                    </destination>
                    <descr><![CDATA[NAT Port Forward to 192.168.13.17 Pf]]></descr>
                    <associated-rule-id>nat_57c01787b4e891.75909166</associated-rule-
id>
                    <tracker>1472206727</tracker>
                    <created>
                        <time>1472206727</time>
                        <username>NAT Port Forward</username>
                    </created>
                </rule>
                <rule>
                    <source>
                        <any/>
                    </source>
```

```
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                                <address>192.168.13.18</address>
                                <port>80</port>
                        </destination>
                        <descr><![CDATA[NAT Port Forward to 192.168.13.18 Pf]]></descr>
                        <associated-rule-id>nat_57c017be3dffa1.16882401</associated-rule-
id>
                        <tracker>1472206782</tracker>
                        <created>
                                <time>1472206782</time>
                                <username>NAT Port Forward</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                                <address>192.168.13.19</address>
                                <port>80</port>
                        </destination>
                        <descr><![CDATA[NAT Port Forward to 192.168.13.19 Pf]]></descr>
                        <associated-rule-id>nat_57c017e1e48d65.86612217</associated-rule-
id>
                        <tracker>1472206817</tracker>
                        <created>
                                <time>1472206817</time>
                                <username>NAT Port Forward</username>
                        </created>
                </rule>
                <rule>
```

```
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                                <address>192.168.13.20</address>
                                <port>80</port>
                        </destination>
                        <descr><![CDATA[NAT Port Forward to 192.168.13.20 Pf]]></descr>
                        <associated-rule-id>nat_57c0187fd4a074.12397754</associated-rule-
id>
                        <tracker>1472206975</tracker>
                        <created>
                                <time>1472206975</time>
                                <username>NAT Port Forward</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                                <address>192.168.17.10</address>
                                <port>8000</port>
                        </destination>
                        <descr><![CDATA[NAT Splunk port 8000 Web Interface]]></descr>
                        <associated-rule-id>nat_57d825ba865df6.65796295</associated-rule-
id>
                        <tracker>1473783226</tracker>
                        <created>
                                <time>1473783226</time>
                                <username>NAT Port Forward</username>
```

```
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                                <address>192.168.19.11</address>
                                <port>22</port>
                        </destination>
                        <descr><![CDATA[NAT Port forward to openldap; ]]></descr>
                        <associated-rule-id>nat_57f555406f2de3.01889708</associated-rule-
id>
                        <tracker>1475695936</tracker>
                        <created>
                                <time>1475695936</time>
                                <username>NAT Port Forward</username>
                        </created>
                </rule>
                <rule>
                        <source>
                                <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp</protocol>
                        <destination>
                                <address>192.168.13.130</address>
                                <port>80</port>
                        </destination>
                        <descr><![CDATA[NAT Mapping to pfsense 192.168.13.130]]></descr>
                        <associated-rule-id>nat_581795efbc2944.51341500</associated-rule-
id>
                        <tracker>1477940719</tracker>
```

```
                        <created>
                              <time>1477940719</time>
                              <username>NAT Port Forward</username>
                        </created>
                  </rule>
                  <rule>
                        <source>
                              <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                              <address>192.168.17.10</address>
                              <port>22</port>
                        </destination>
                        <descr><![CDATA[NAT Splunk SSH ]]></descr>
                        <associated-rule-id>nat_582ef78ed63d23.63868026</associated-rule-
id>
                        <tracker>1479473038</tracker>
                        <created>
                              <time>1479473038</time>
                              <username>NAT Port Forward</username>
                        </created>
                  </rule>
                  <rule>
                        <source>
                              <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
                              <address>192.168.20.6</address>
                              <port>443</port>
                        </destination>
```

```
                    <descr><![CDATA[NAT Port Forward to Hytrust Cloud Control
192.168.20.6]]></descr>
                    <associated-rule-id>nat_585ab274d8bce0.68941358</associated-rule-
id>
                    <tracker>1482338932</tracker>
                    <created>
                          <time>1482338932</time>
                          <username>NAT Port Forward</username>
                    </created>
             </rule>
             <rule>
                    <id/>
                    <tracker>1480540738</tracker>
                    <type>pass</type>
                    <interface>lan</interface>
                    <ipprotocol>inet</ipprotocol>
                    <tag/>
                    <tagged/>
                    <max/>
                    <max-src-nodes/>
                    <max-src-conn/>
                    <max-src-states/>
                    <statetimeout/>
                    <statetype>keep state</statetype>
                    <os/>
                    <source>
                          <any/>
                    </source>
                    <destination>
                          <any/>
                    </destination>
                    <descr><![CDATA[Allow all LAN traffic to go to anywhere]]></descr>
                    <updated>
                          <time>1480540738</time>
                          <username>admin@10.97.67.140</username>
```

```
3811                    </updated>
3812                    <created>
3813                            <time>1480540738</time>
3814                            <username>admin@10.97.67.140</username>
3815                    </created>
3816            </rule>
3817            <rule>
3818                    <id/>
3819                    <tracker>1465934857</tracker>
3820                    <type>pass</type>
3821                    <interface>lan</interface>
3822                    <ipprotocol>inet</ipprotocol>
3823                    <tag/>
3824                    <tagged/>
3825                    <max/>
3826                    <max-src-nodes/>
3827                    <max-src-conn/>
3828                    <max-src-states/>
3829                    <statetimeout/>
3830                    <statetype>keep state</statetype>
3831                    <os/>
3832                    <protocol>icmp</protocol>
3833                    <source>
3834                            <any/>
3835                    </source>
3836                    <destination>
3837                            <any/>
3838                    </destination>
3839                    <descr/>
3840                    <updated>
3841                            <time>1465934857</time>
3842                            <username>admin@192.168.13.101</username>
3843                    </updated>
3844                    <created>
```

```
3845                        <time>1465934857</time>
3846                        <username>admin@192.168.13.101</username>
3847                  </created>
3848            </rule>
3849            <rule>
3850                  <type>pass</type>
3851                  <ipprotocol>inet</ipprotocol>
3852                  <descr><![CDATA[Default allow LAN to any rule]]></descr>
3853                  <interface>lan</interface>
3854                  <tracker>0100000101</tracker>
3855                  <source>
3856                        <network>lan</network>
3857                  </source>
3858                  <destination>
3859                        <any/>
3860                  </destination>
3861            </rule>
3862            <rule>
3863                  <type>pass</type>
3864                  <ipprotocol>inet6</ipprotocol>
3865                  <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
3866                  <interface>lan</interface>
3867                  <tracker>0100000102</tracker>
3868                  <source>
3869                        <network>lan</network>
3870                  </source>
3871                  <destination>
3872                        <any/>
3873                  </destination>
3874            </rule>
3875            <rule>
3876                  <id/>
3877                  <tracker>1476720530</tracker>
3878                  <type>pass</type>
```

```
                        <interface>enc0</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <source>
                              <any/>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                        <descr><![CDATA[Allow  All traffic sourced from Tunnel to Anywhere
o]]></descr>
                        <created>
                              <time>1476720530</time>
                              <username>admin@10.97.67.137</username>
                        </created>
                        <updated>
                              <time>1476720628</time>
                              <username>admin@10.97.67.137</username>
                        </updated>
                  </rule>
                  <separator>
                        <lan/>
                        <wan/>
                        <floatingrules/>
                        <enc0/>
                  </separator>
```

```
3913                <bypassstaticroutes>yes</bypassstaticroutes>
3914          </filter>
3915          <shaper/>
3916          <ipsec>
3917                <phase1>
3918                      <ikeid>1</ikeid>
3919                      <iketype>ikev1</iketype>
3920                      <mode>main</mode>
3921                      <interface>wan</interface>
3922                      <remote-gateway>174.47.13.99</remote-gateway>
3923                      <protocol>inet</protocol>
3924                      <myid_type>myaddress</myid_type>
3925                      <myid_data/>
3926                      <peerid_type>peeraddress</peerid_type>
3927                      <peerid_data/>
3928                      <encryption-algorithm>
3929                            <name>aes</name>
3930                            <keylen>256</keylen>
3931                      </encryption-algorithm>
3932                      <hash-algorithm>sha1</hash-algorithm>
3933                      <dhgroup>2</dhgroup>
3934                      <lifetime>28800</lifetime>
3935                      <pre-shared-key>78J%3AkmP*Krr294xYE=v@</pre-shared-key>
3936                      <private-key/>
3937                      <certref/>
3938                      <caref/>
3939                      <authentication_method>pre_shared_key</authentication_method>
3940                      <descr><![CDATA[IPSEC IKEv1 Tunnel to Vanguard's Firewall Public
3941 IP address]]></descr>
3942                      <nat_traversal>force</nat_traversal>
3943                      <mobike>off</mobike>
3944                      <dpd_delay>10</dpd_delay>
3945                      <dpd_maxfail>5</dpd_maxfail>
3946                </phase1>
```

```
<client/>
<phase2>
	<ikeid>1</ikeid>
	<uniqid>5804f45c4f196</uniqid>
	<mode>tunnel</mode>
	<reqid>1</reqid>
	<localid>
		<type>network</type>
		<address>192.168.19.0</address>
		<netbits>24</netbits>
	</localid>
	<remoteid>
		<type>network</type>
		<address>172.17.212.0</address>
		<netbits>24</netbits>
	</remoteid>
	<protocol>esp</protocol>
	<encryption-algorithm-option>
		<name>aes</name>
		<keylen>256</keylen>
	</encryption-algorithm-option>
	<hash-algorithm-option>hmac_sha1</hash-algorithm-option>
	<pfsgroup>0</pfsgroup>
	<lifetime>3600</lifetime>
	<pinghost/>
	<descr><![CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
</phase2>
<phase2>
	<ikeid>1</ikeid>
	<uniqid>586d5ecf7f516</uniqid>
	<mode>tunnel</mode>
	<reqid>2</reqid>
	<localid>
		<type>network</type>
```

```
                        <address>192.168.17.0</address>
                        <netbits>24</netbits>
                </localid>
                <remoteid>
                        <type>network</type>
                        <address>172.17.212.0</address>
                        <netbits>24</netbits>
                </remoteid>
                <protocol>esp</protocol>
                <encryption-algorithm-option>
                        <name>aes</name>
                        <keylen>256</keylen>
                </encryption-algorithm-option>
                <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
                <pfsgroup>0</pfsgroup>
                <lifetime>3600</lifetime>
                <pinghost/>
                <descr><![CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
        </phase2>
        <phase2>
                <ikeid>1</ikeid>
                <uniqid>586d5eeb02957</uniqid>
                <mode>tunnel</mode>
                <reqid>3</reqid>
                <localid>
                        <type>network</type>
                        <address>192.168.13.0</address>
                        <netbits>24</netbits>
                </localid>
                <remoteid>
                        <type>network</type>
                        <address>172.17.212.0</address>
                        <netbits>24</netbits>
                </remoteid>
```

```
                <protocol>esp</protocol>
                <encryption-algorithm-option>
                        <name>aes</name>
                        <keylen>256</keylen>
                </encryption-algorithm-option>
                <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
                <pfsgroup>0</pfsgroup>
                <lifetime>3600</lifetime>
                <pinghost/>
                <descr><![CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
        </phase2>
        <phase2>
                <ikeid>1</ikeid>
                <uniqid>586d5f54943b4</uniqid>
                <mode>tunnel</mode>
                <reqid>4</reqid>
                <localid>
                        <type>network</type>
                        <address>192.168.14.0</address>
                        <netbits>24</netbits>
                </localid>
                <remoteid>
                        <type>network</type>
                        <address>172.17.212.0</address>
                        <netbits>24</netbits>
                </remoteid>
                <protocol>esp</protocol>
                <encryption-algorithm-option>
                        <name>aes</name>
                        <keylen>256</keylen>
                </encryption-algorithm-option>
                <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
                <pfsgroup>0</pfsgroup>
                <lifetime>3600</lifetime>
```

```
                    <pinghost/>
                    <descr><![CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
             </phase2>
      </ipsec>
      <aliases/>
      <proxyarp/>
      <cron>
             <item>
                    <minute>1,31</minute>
                    <hour>0-5</hour>
                    <mday>*</mday>
                    <month>*</month>
                    <wday>*</wday>
                    <who>root</who>
                    <command>/usr/bin/nice -n20 adjkerntz -a</command>
             </item>
             <item>
                    <minute>1</minute>
                    <hour>3</hour>
                    <mday>1</mday>
                    <month>*</month>
                    <wday>*</wday>
                    <who>root</who>
                    <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
             </item>
             <item>
                    <minute>*/60</minute>
                    <hour>*</hour>
                    <mday>*</mday>
                    <month>*</month>
                    <wday>*</wday>
                    <who>root</who>
                    <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
sshlockout</command>
```

```
4083                </item>
4084                <item>
4085                        <minute>*/60</minute>
4086                        <hour>*</hour>
4087                        <mday>*</mday>
4088                        <month>*</month>
4089                        <wday>*</wday>
4090                        <who>root</who>
4091                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4092 webConfiguratorlockout</command>
4093                </item>
4094                <item>
4095                        <minute>1</minute>
4096                        <hour>1</hour>
4097                        <mday>*</mday>
4098                        <month>*</month>
4099                        <wday>*</wday>
4100                        <who>root</who>
4101                        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
4102                </item>
4103                <item>
4104                        <minute>*/60</minute>
4105                        <hour>*</hour>
4106                        <mday>*</mday>
4107                        <month>*</month>
4108                        <wday>*</wday>
4109                        <who>root</who>
4110                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4111 virusprot</command>
4112                </item>
4113                <item>
4114                        <minute>30</minute>
4115                        <hour>12</hour>
4116                        <mday>*</mday>
4117                        <month>*</month>
```

```
                <wday>*</wday>
                <who>root</who>
                <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
        </item>
</cron>
<wol/>
<rrd>
        <enable/>
</rrd>
<load_balancer>
        <monitor_type>
                <name>ICMP</name>
                <type>icmp</type>
                <descr><![CDATA[ICMP]]></descr>
                <options/>
        </monitor_type>
        <monitor_type>
                <name>TCP</name>
                <type>tcp</type>
                <descr><![CDATA[Generic TCP]]></descr>
                <options/>
        </monitor_type>
        <monitor_type>
                <name>HTTP</name>
                <type>http</type>
                <descr><![CDATA[Generic HTTP]]></descr>
                <options>
                        <path>/</path>
                        <host/>
                        <code>200</code>
                </options>
        </monitor_type>
        <monitor_type>
                <name>HTTPS</name>
```

```
                        <type>https</type>
                        <descr><![CDATA[Generic HTTPS]]></descr>
                        <options>
                              <path>/</path>
                              <host/>
                              <code>200</code>
                        </options>
                  </monitor_type>
                  <monitor_type>
                        <name>SMTP</name>
                        <type>send</type>
                        <descr><![CDATA[Generic SMTP]]></descr>
                        <options>
                              <send/>
                              <expect>220 *</expect>
                        </options>
                  </monitor_type>
            </load_balancer>
            <widgets>

            <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
/sequence>
            </widgets>
            <openvpn/>
            <dnshaper/>
            <unbound>
                  <enable/>
                  <dnssec/>
                  <active_interface/>
                  <outgoing_interface/>
                  <custom_options/>
                  <hideidentity/>
                  <hideversion/>
                  <dnssecstripped/>
            </unbound>
```

```
        <dhcpdv6>
                <lan>
                        <range>
                                <from>::1000</from>
                                <to>::2000</to>
                        </range>
                        <ramode>assist</ramode>
                        <rapriority>medium</rapriority>
                </lan>
        </dhcpdv6>
        <cert>
                <refid>5720a0502b277</refid>
                <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
                <type>server</type>

        <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXZ0F3SUJBZ0lCQURBTkJna3
Foa2lHOXcwQkFRc0ZBRENCdERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnTlZCQWdUQlZOMFlYUmxNUkV3RHdZ
RFZRUUhFd2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApaVzV6WlNCM1pXSkRiMjVtYVdkMWNtRjBiM0
lnVTJWc1ppMVRhV2R1WldRZ1EyVnlkR2xtYVdOaGRHVXhLREFtCkJna3Foa2lHOXcwQkNRRVdHV0ZrYldsdVFI
Qm1VMlZ1YzJVdWJHOWpZV3hrYjIxaGFXNHhIakFjQmdOVkJBTVQKRlhCbVUyVnVjMlV0TlRjeU1HRXdOVEF5WW
pJM056QWVGdzB4TmpBME1qY3hNVEU1TkRSYUZ3MHlNVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
d0pWVXpFT01Bd0dBMVVFQ0JNRlUzUmhkR1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNU1UZ3dOZ1lEVlFRS0
V5OXdabE5sYm5ObElZGxZa052Ym1acFozVnlZWFJ2Y2lCVFpXeG0KTFZOcFoyNWxaQ0JEWlhKMGFXWnBZMkYw
WlRFb01DWUdDU3FHU0liM0RRRUpBUllaWVdSdGFXNUFjR1pUWlc1egpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
dBMVVFQXhNVmNHWlRaVzV6WlMwMU56SXdZVEExTURKaU1qYzNNSUlCCklqQU5CZ2txaGtpRzl3MEJBUUVGQUFP
Q0FROEFNSUlCQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
hDODBHU0dhZnJENWdqcTRwZkNNMHlzbEFPaVlZK1hDYjdNa2o0dmtTMgpmbzl4emNyaDUrNVlaYlBHeXR1a2ls
ZWR4bjFWeFl6SllzYXZKdnlKb1lRMCtNTkx0dkFjYnRhTUFoZjh1ZkRFClhrclNVQ0N5YTFrbEYxNWJGZmcyUG
E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkUFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXd1SEZwd3J1LytYWExieEcrcD
dwYXI0aHR0UFRDcml1NmFqQVVTNmpvN05kOElQNWpzZ1kzR0h2ZjhzUUlECkFRQUJvNElCaGpDQ0FZSXdDUVlE
VlIwVEJBSXdBREFSQmdsZ2hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWkkKQVliNFFnRU5CQ1lXSkU5d1pXNV
RVMHdnUjJWdVpYSmhkR1ZrSUZObGNuWmxjaUJEWlhKMGFXWnBZMkYwWlRBZApCZ05WSFE0RUZnUVU3K1lLRmNp
OFFVSGhTZ0xEdjhFQ3NjQ0p3QUl3Z2VFR0ExVWRJd1NCMlRDQjFvQVU3K1lLCkZjaThRVUhoU2dMRHY4RUNzY0
NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsVlRNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
VUVCeE1JVEc5allXeHBkSGt4T0RBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaQpRMjl1Wm1sbmRYSmhkRzl5SU
ZObGJHWXRVMmxuYm1Wa0lFTmxjblJwWm1sallYUmxNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
bE5sYm5ObExteHZZMkZzZWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
56ZUNBUUF3SFFZRFZSMGxCQll3RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd0lG
b0RBTkJna3Foa2lHOXcwQkFRc0ZBQU9DVFFQXJxZFpQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmtNaTB5M0
9PWGtzWEs1cEM2dTd6Ukl3WjEvRjYyRUp3ODlUOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWJhRU42NEkxOHFud3Zm
S2JrREZvRThMR1hSdzBkMnAyTGVmYTd4YTIvSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG
c4bGdrcVc3dStlb01DNDJIbVJkOURCTmlzdFJ4RVlNMkFLQkFsZG1LYStvRUY1VUwwCm43aXpvNlZ4dHJWMTJv
TTdySllRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VVnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOVpPSmR2QmZLVU
1sUWlELyswSVpTalFXRDczWkdsaEhTK2tOeWc1aDJhUjUwYjh3Wm9zQnNjSUZDa0pFbgp0UT09Ci0tLS0tRU5E
IENFUlRJRklDQVRFLS0tLS0K</crt>

        <prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z0lCQURBTkJna3Foa2lHOXcwQkFRRU
ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M0lhYlkKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4
```

```
eGxiY3UyRUx6UVpJWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMWitqM0hOeXVIbjdsaGxzOG
JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcwdTI4Qnh1CjFvd0NGL3k1OE1SZVN0SlFJTEpyV1NVWFhs
c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcwdkEKQVdEQkQzNDg5OHRUalhROVNpb1NaclREEbn
dKTmo3cHAwQnM4ZHhlRDBjL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
dHZFYjZudWxxdmlHMjA5TUt1SzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUpRRF
pxU3duMnNTUTh0SVNBTUVrUW0zcXhrb3BzdzB4cWNScmFlOEd4VmQKejBpOU1KbkZVQWFleTQvL3Jldndh ZW1P
R3RYSmZ2ai9jSnY3cmJIWGIzYkJtVW9hcDhxY0RjdnVSMmlHRUZYWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcD
lzNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1ZnlP
UzAvbXlmNU5YLzVoRklPNmFDc0xlUjZ4N1RZa2FDQU9FYlViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
hMZ0NRYlB2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUE0NzNMUWoxcExLSmRZN2JxCmtMU3NVT0ZhTUZlZG1xU2ttbzh3Qj
lpMXhzbElLQUd0M3U4dTdMZlZtU2lybnMwVVBTMHRVUDRyQXMzVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
OGttbFJnUFRmVHVPaGNwMGVkamQwK1E5Y2VlY25kaFp3UEl6TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHNhbm
NBRDhVYThDZ1lFQXpzYjYzbzRBSHlYNjZkcEJ6TGlzYzZxS2d2ZG4xazhVCm02N3RuK2M3NkVhSEtZTlk0Rjdh
S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUpOK0I3Sm
Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZm1DWlpRSUQ1OENnWUJjamFO
dk5obnFJOG9rWGhBUjR2c3NtNGpWb0tYU1ZScjRIVHo5MDFwOGdReXNCWkt0CnlUS2V6VThuUVZvTjNYWmVMbC
8rVEcwYVpKOTZHKy9nNTRWZmZqWTRlelVScHhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
QWY5Mi9CbHZJR25FS1pMdnhLWTdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
RG1hZGsvKy9Ud2UvVk1Kbmx2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUjlhbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBRS0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1Rlczdu
WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLClUzSThhYnpnUUtwOEwrZj
VadTAxY1pZVk5TU0FIUFRHYm5jb1IzbGVPYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>
```


```
        </cert>
        <revision>
                <time>1493217875</time>
                <description><![CDATA[admin@10.97.67.148: /firewall_nat_1to1_edit.php
made unknown change]]></description>
                <username>admin@10.97.67.148</username>
        </revision>
        <gateways>
                <gateway_item>
                        <interface>wan</interface>
                        <gateway>10.33.50.33</gateway>
                        <name>GW_WAN</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <interval/>
                        <descr><![CDATA[Interface wan Gateway]]></descr>
                        <defaultgw/>
                </gateway_item>
                <gateway_item>
                        <interface>lan</interface>
```

```
                <gateway>192.168.13.14</gateway>
                <name>VLAN2014</name>
                <weight>1</weight>
                <ipprotocol>inet</ipprotocol>
                <descr/>
        </gateway_item>
        <gateway_item>
                <interface>lan</interface>
                <gateway>192.168.13.19</gateway>
                <name>VLAN2019</name>
                <weight>1</weight>
                <ipprotocol>inet</ipprotocol>
                <descr><![CDATA[VLAN2019]]></descr>
        </gateway_item>
        <gateway_item>
                <interface>lan</interface>
                <gateway>192.168.13.18</gateway>
                <name>VLAN2018</name>
                <weight>1</weight>
                <ipprotocol>inet</ipprotocol>
                <descr><![CDATA[VLAN2018]]></descr>
        </gateway_item>
        <gateway_item>
                <interface>lan</interface>
                <gateway>192.168.13.15</gateway>
                <name>VLAN2015</name>
                <weight>1</weight>
                <ipprotocol>inet</ipprotocol>
                <descr/>
        </gateway_item>
        <gateway_item>
                <interface>lan</interface>
                <gateway>192.168.13.16</gateway>
                <name>VLAN2016</name>
```

```
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr/>
                </gateway_item>
                <gateway_item>
                        <interface>lan</interface>
                        <gateway>192.168.13.17</gateway>
                        <name>VLAN2017</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr/>
                </gateway_item>
                <gateway_item>
                        <interface>lan</interface>
                        <gateway>192.168.13.20</gateway>
                        <name>VLAN2020</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr/>
                </gateway_item>
                <gateway_item>
                        <interface>lan</interface>
                        <gateway>192.168.13.10</gateway>
                        <name>VLAN2066</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr><![CDATA[Gateway to Vendor Net]]></descr>
                </gateway_item>
        </gateways>
        <ppps/>
        <dyndnses/>
        <virtualip>
                <vip>
                        <mode>ipalias</mode>
```

```
                <interface>wan</interface>
                <uniqid>576b23658af3d</uniqid>
                <descr><![CDATA[Virtual IP for Splunk]]></descr>
                <type>single</type>
                <subnet_bits>32</subnet_bits>
                <subnet>10.33.50.35</subnet>
        </vip>
        <vip>
                <mode>ipalias</mode>
                <interface>wan</interface>
                <uniqid>5773d4c39ae54</uniqid>
                <descr><![CDATA[Virtual IP for RadiantOne VDS]]></descr>
                <type>single</type>
                <subnet_bits>32</subnet_bits>
                <subnet>10.33.50.37</subnet>
        </vip>
        <vip>
                <mode>ipalias</mode>
                <interface>wan</interface>
                <uniqid>57a8ce7868f78</uniqid>
                <descr><![CDATA[Virtual IP for Hytrust ESXi Server]]></descr>
                <type>single</type>
                <subnet_bits>32</subnet_bits>
                <subnet>10.33.50.36</subnet>
        </vip>
        <vip>
                <mode>ipalias</mode>
                <interface>wan</interface>
                <uniqid>57aa0a09a4d09</uniqid>
                <descr><![CDATA[VIP for Hytrust CloudControl VM]]></descr>
                <type>single</type>
                <subnet_bits>32</subnet_bits>
                <subnet>10.33.50.38</subnet>
        </vip>
```

```
        <vip>
                <mode>ipalias</mode>
                <interface>wan</interface>
                <uniqid>57b615eac1f16</uniqid>
                <descr><![CDATA[VIP for VCenter Server]]></descr>
                <type>single</type>
                <subnet_bits>32</subnet_bits>
                <subnet>10.33.50.39</subnet>
        </vip>
        <vip>
                <mode>ipalias</mode>
                <interface>wan</interface>
                <uniqid>57bd089e9ab62</uniqid>
                <descr><![CDATA[VIP for ActiveDirectory]]></descr>
                <type>single</type>
                <subnet_bits>32</subnet_bits>
                <subnet>10.33.50.40</subnet>
        </vip>
        <vip>
                <mode>ipalias</mode>
                <interface>wan</interface>
                <uniqid>57bf0bbc594c5</uniqid>
                <descr><![CDATA[VIP for  OpenLDAP]]></descr>
                <type>single</type>
                <subnet_bits>32</subnet_bits>
                <subnet>10.33.50.41</subnet>
        </vip>
        <vip>
                <mode>ipalias</mode>
                <interface>wan</interface>
                <uniqid>57bf97481ae8c</uniqid>
                <descr><![CDATA[VIP for Internal Pfsense Firewalls]]></descr>
                <type>single</type>
                <subnet_bits>32</subnet_bits>
```

```
                        <subnet>10.33.50.42</subnet>
                </vip>
                <vip>
                        <mode>ipalias</mode>
                        <interface>wan</interface>
                        <uniqid>581788c622d42</uniqid>
                        <descr><![CDATA[VIP for ConsoleWorks -- Mapping to Internal
Address]]></descr>
                        <type>single</type>
                        <subnet_bits>32</subnet_bits>
                        <subnet>10.33.50.43</subnet>
                </vip>
                <vip>
                        <mode>ipalias</mode>
                        <interface>wan</interface>
                        <uniqid>58179833f127e</uniqid>
                        <descr><![CDATA[Testing ]]></descr>
                        <type>single</type>
                        <subnet_bits>32</subnet_bits>
                        <subnet>10.33.50.44</subnet>
                </vip>
                <vip>
                        <mode>ipalias</mode>
                        <interface>wan</interface>
                        <uniqid>58e410a9241f1</uniqid>
                        <descr><![CDATA[Mapping to CentOSToAD VM (test machine)]]></descr>
                        <type>single</type>
                        <subnet_bits>32</subnet_bits>
                        <subnet>10.33.50.45</subnet>
                </vip>
                <vip>
                        <mode>ipalias</mode>
                        <interface>wan</interface>
                        <uniqid>5900b1ef3b079</uniqid>
```

```
                    <descr><![CDATA[AlertEnterprise Enterprise Guardian]]></descr>
                    <type>single</type>
                    <subnet_bits>32</subnet_bits>
                    <subnet>10.33.50.46</subnet>
             </vip>
      </virtualip>
</pfSense>
```

2.10.2 Firewall Configuration for Common Services Subnet

```
<?xml version="1.0"?>
<pfSense>
      <version>15.4</version>
      <lastchange/>
      <theme>pfSense_ng</theme>
      <system>
            <optimization>normal</optimization>
            <hostname>FS-ARM</hostname>
            <domain>FS-ARM.gov</domain>
            <group>
                  <name>all</name>
                  <description><![CDATA[All Users]]></description>
                  <scope>system</scope>
                  <gid>1998</gid>
                  <member>0</member>
            </group>
            <group>
                  <name>admins</name>
                  <description><![CDATA[System Administrators]]></description>
                  <scope>system</scope>
                  <gid>1999</gid>
                  <member>0</member>
                  <priv>page-all</priv>
            </group>
            <user>
                  <name>admin</name>
```

```
                <descr><![CDATA[System Administrator]]></descr>
                <scope>system</scope>
                <groupname>admins</groupname>
                <password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
                <uid>0</uid>
                <priv>user-shell-access</priv>
        </user>
        <nextuid>2000</nextuid>
        <nextgid>2000</nextgid>
        <timezone>America/New_York</timezone>
        <time-update-interval/>
        <timeservers>10.97.74.8</timeservers>
        <webgui>
                <protocol>http</protocol>
                <loginautocomplete/>
                <ssl-certref>5720a0502b277</ssl-certref>
                <dashboardcolumns>2</dashboardcolumns>
                <port/>
                <max_procs>2</max_procs>
                <nohttpreferercheck/>
        </webgui>
        <disablenatreflection>yes</disablenatreflection>
        <disablesegmentationoffloading/>
        <disablelargereceiveoffloading/>
        <ipv6allow/>
        <powerd_ac_mode>hadp</powerd_ac_mode>
        <powerd_battery_mode>hadp</powerd_battery_mode>
        <powerd_normal_mode>hadp</powerd_normal_mode>
        <bogons>
                <interval>monthly</interval>
        </bogons>
        <language>en_US</language>
        <dns1gw>GW_WAN</dns1gw>
        <dns2gw>GW_WAN</dns2gw>
```

```
4519                <dns3gw>none</dns3gw>
4520                <dns4gw>none</dns4gw>
4521                <dnsserver>10.97.74.8</dnsserver>
4522                <dnsserver>10.63.255.2</dnsserver>
4523                <maximumstates/>
4524                <aliasesresolveinterval/>
4525                <maximumtableentries/>
4526                <maximumfrags/>
4527                <reflectiontimeout/>
4528                <serialspeed>115200</serialspeed>
4529                <primaryconsole>serial</primaryconsole>
4530          </system>
4531          <interfaces>
4532                <wan>
4533                      <if>em0</if>
4534                      <descr><![CDATA[WAN]]></descr>
4535                      <enable/>
4536                      <spoofmac/>
4537                      <ipaddr>192.168.13.19</ipaddr>
4538                      <subnet>24</subnet>
4539                      <gateway>GW_WAN_2</gateway>
4540                      <ipaddrv6/>
4541                      <subnetv6/>
4542                      <gatewayv6/>
4543                </wan>
4544                <lan>
4545                      <enable/>
4546                      <if>em1</if>
4547                      <ipaddr>192.168.19.1</ipaddr>
4548                      <subnet>24</subnet>
4549                      <ipaddrv6/>
4550                      <subnetv6/>
4551                      <media/>
4552                      <mediaopt/>
```

```
                    <track6-interface>wan</track6-interface>
                    <track6-prefix-id>0</track6-prefix-id>
                    <gateway/>
                    <gatewayv6/>
             </lan>
      </interfaces>
      <staticroutes>
             <route>
                    <network>192.168.17.0/24</network>
                    <gateway>GW_VLAN17</gateway>
                    <descr><![CDATA[Route to VLAN 17]]></descr>
             </route>
      </staticroutes>
      <dhcpd>
             <lan>
                    <enable/>
                    <range>
                           <from>192.168.19.100</from>
                           <to>192.168.19.150</to>
                    </range>
             </lan>
             <opt1>
                    <enable/>
                    <range>
                           <from>192.168.14.100</from>
                           <to>192.168.14.150</to>
                    </range>
             </opt1>
             <opt2>
                    <enable/>
                    <range>
                           <from>192.168.15.100</from>
                           <to>192.168.15.150</to>
                    </range>
```

```
4587                </opt2>
4588                <opt3>
4589                        <enable/>
4590                        <range>
4591                                <from>192.168.16.100</from>
4592                                <to>192.168.16.150</to>
4593                        </range>
4594                </opt3>
4595        </dhcpd>
4596        <snmpd>
4597                <syslocation/>
4598                <syscontact/>
4599                <rocommunity>public</rocommunity>
4600        </snmpd>
4601        <diag>
4602                <ipv6nat>
4603                        <ipaddr/>
4604                </ipv6nat>
4605        </diag>
4606        <bridge/>
4607        <syslog/>
4608        <nat>
4609                <outbound>
4610                        <mode>disabled</mode>
4611                </outbound>
4612        </nat>
4613        <filter>
4614                <rule>
4615                        <id/>
4616                        <tracker>1493319263</tracker>
4617                        <type>pass</type>
4618                        <interface>wan</interface>
4619                        <ipprotocol>inet</ipprotocol>
4620                        <tag/>
```

```
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                </destination>
                <descr><![CDATA[Allow Any to LAN net]]></descr>
                <updated>
                        <time>1493319263</time>
                        <username>admin@10.97.67.143</username>
                </updated>
                <created>
                        <time>1493319263</time>
                        <username>admin@10.97.67.143</username>
                </created>
                <disabled/>
        </rule>
        <rule>
                <id/>
                <tracker>1481038226</tracker>
                <type>pass</type>
                <interface>wan</interface>
```

```
4655                    <ipprotocol>inet</ipprotocol>
4656                    <tag/>
4657                    <tagged/>
4658                    <direction>any</direction>
4659                    <quick>yes</quick>
4660                    <floating>yes</floating>
4661                    <max/>
4662                    <max-src-nodes/>
4663                    <max-src-conn/>
4664                    <max-src-states/>
4665                    <statetimeout/>
4666                    <statetype>keep state</statetype>
4667                    <os/>
4668                    <source>
4669                           <address>192.168.14.111</address>
4670                    </source>
4671                    <destination>
4672                           <any/>
4673                    </destination>
4674                    <disabled/>
4675                    <descr><![CDATA[Allow Radiant (192.168.14.111) in -WAN]]></descr>
4676                    <created>
4677                           <time>1481038226</time>
4678                           <username>admin@10.97.67.155</username>
4679                    </created>
4680                    <updated>
4681                           <time>1493311659</time>
4682                           <username>admin@10.97.67.143</username>
4683                    </updated>
4684             </rule>
4685             <rule>
4686                    <id/>
4687                    <tracker>1481038269</tracker>
4688                    <type>pass</type>
```

```
4689                    <interface>wan</interface>
4690                    <ipprotocol>inet</ipprotocol>
4691                    <tag/>
4692                    <tagged/>
4693                    <direction>any</direction>
4694                    <quick>yes</quick>
4695                    <floating>yes</floating>
4696                    <max/>
4697                    <max-src-nodes/>
4698                    <max-src-conn/>
4699                    <max-src-states/>
4700                    <statetimeout/>
4701                    <statetype>keep state</statetype>
4702                    <os/>
4703                    <protocol>tcp/udp</protocol>
4704                    <source>
4705                           <any/>
4706                    </source>
4707                    <destination>
4708                           <network>lan</network>
4709                           <port>389</port>
4710                    </destination>
4711                    <descr><![CDATA[Allow LDAP traffic to AD and OpenLDAP]]></descr>
4712                    <created>
4713                           <time>1481038269</time>
4714                           <username>admin@10.97.67.155</username>
4715                    </created>
4716                    <updated>
4717                           <time>1493319675</time>
4718                           <username>admin@10.97.67.143</username>
4719                    </updated>
4720             </rule>
4721             <rule>
4722                    <id/>
```

```
                        <tracker>1493314739</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp/udp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <any/>
                                <port>636</port>
                        </destination>
                        <descr><![CDATA[Allow Connection to LDAPS on AD and
OpenLDAP]]></descr>
                        <created>
                                <time>1493314739</time>
                                <username>admin@10.97.67.143</username>
                        </created>
                        <updated>
                                <time>1493319543</time>
                                <username>admin@10.97.67.143</username>
                        </updated>
```

```
4757                <rule>
4758                <rule>
4759                      <id/>
4760                      <tracker>1472179541</tracker>
4761                      <type>pass</type>
4762                      <interface>wan</interface>
4763                      <ipprotocol>inet</ipprotocol>
4764                      <tag/>
4765                      <tagged/>
4766                      <direction>any</direction>
4767                      <quick>yes</quick>
4768                      <floating>yes</floating>
4769                      <max/>
4770                      <max-src-nodes/>
4771                      <max-src-conn/>
4772                      <max-src-states/>
4773                      <statetimeout/>
4774                      <statetype>keep state</statetype>
4775                      <os/>
4776                      <protocol>tcp/udp</protocol>
4777                      <source>
4778                            <any/>
4779                      </source>
4780                      <destination>
4781                            <any/>
4782                      </destination>
4783                      <disabled/>
4784                      <descr><![CDATA[Testing to see if there will be communication
4785 betwee]]></descr>
4786                      <created>
4787                            <time>1472179541</time>
4788                            <username>admin@192.168.13.135</username>
4789                      </created>
4790                      <updated>
```

```
                        <time>1493311684</time>
                        <username>admin@10.97.67.143</username>
                </updated>
        </rule>
        <rule>
                <id/>
                <tracker>1493327079</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>icmp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                </destination>
                <descr><![CDATA[Allow ICMP for troubleshooting]]></descr>
                <updated>
                        <time>1493327079</time>
                        <username>admin@10.97.67.143</username>
                </updated>
```

```
                        <created>
                                <time>1493327079</time>
                                <username>admin@10.97.67.143</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1493327306</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os></os>
                        <protocol>tcp/udp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <any/>
                                <port>53</port>
                        </destination>
                        <descr><![CDATA[Allow DNS Requests to AD]]></descr>
                        <updated>
                                <time>1493327306</time>
```

```
                        <username>admin@10.97.67.143</username>
                </updated>
                <created>
                        <time>1493327306</time>
                        <username>admin@10.97.67.143</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493312171</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                        <port>389</port>
                </destination>
                <descr><![CDATA[Allow LDAP traffic to LAN nodes]]></descr>
                <updated>
                        <time>1493312171</time>
                        <username>admin@10.97.67.143</username>
```

```
                </updated>
                <created>
                        <time>1493312171</time>
                        <username>admin@10.97.67.143</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493313314</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                        <port>53</port>
                </destination>
                <descr><![CDATA[Allow DNS traffic to LAN nodes]]></descr>
                <updated>
                        <time>1493313314</time>
                        <username>admin@10.97.67.143</username>
                </updated>
```

```
4927                    <created>
4928                          <time>1493313314</time>
4929                          <username>admin@10.97.67.143</username>
4930                    </created>
4931              </rule>
4932              <rule>
4933                    <id/>
4934                    <tracker>1493312231</tracker>
4935                    <type>pass</type>
4936                    <interface>wan</interface>
4937                    <ipprotocol>inet</ipprotocol>
4938                    <tag/>
4939                    <tagged/>
4940                    <max/>
4941                    <max-src-nodes/>
4942                    <max-src-conn/>
4943                    <max-src-states/>
4944                    <statetimeout/>
4945                    <statetype>keep state</statetype>
4946                    <os/>
4947                    <protocol>tcp</protocol>
4948                    <source>
4949                          <any/>
4950                    </source>
4951                    <destination>
4952                          <network>lan</network>
4953                          <port>636</port>
4954                    </destination>
4955                    <descr><![CDATA[Allow LDAPs traffic to LAN nodes]]></descr>
4956                    <updated>
4957                          <time>1493312231</time>
4958                          <username>admin@10.97.67.143</username>
4959                    </updated>
4960                    <created>
```

```
                        <time>1493312231</time>
                        <username>admin@10.97.67.143</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493311864</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                        <port>22</port>
                </destination>
                <descr><![CDATA[Allow SSH traffic to LAN nodes ]]></descr>
                <updated>
                        <time>1493311864</time>
                        <username>admin@10.97.67.143</username>
                </updated>
                <created>
                        <time>1493311864</time>
```

```
                        <username>admin@10.97.67.143</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493311502</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <network>lan</network>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr><![CDATA[Allow all LAN traffic to go to anywhere --Applied
to]]></descr>
                <updated>
                        <time>1493311502</time>
                        <username>admin@10.97.67.143</username>
                </updated>
                <created>
                        <time>1493311502</time>
                        <username>admin@10.97.67.143</username>
```

```
                <created>
            </rule>
            <rule>
                <id/>
                <tracker>1493311408</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                    <any/>
                </source>
                <destination>
                    <network>wanip</network>
                    <port>80</port>
                </destination>
                <descr><![CDATA[Allow to Port 80 on Firewall WAN]]></descr>
                <updated>
                    <time>1493311408</time>
                    <username>admin@10.97.67.143</username>
                </updated>
                <created>
                    <time>1493311408</time>
                    <username>admin@10.97.67.143</username>
                </created>
```

```
5063            </rule>
5064            <rule>
5065                    <id/>
5066                    <tracker>1493312279</tracker>
5067                    <type>pass</type>
5068                    <interface>wan</interface>
5069                    <ipprotocol>inet</ipprotocol>
5070                    <tag/>
5071                    <tagged/>
5072                    <max/>
5073                    <max-src-nodes/>
5074                    <max-src-conn/>
5075                    <max-src-states/>
5076                    <statetimeout/>
5077                    <statetype>keep state</statetype>
5078                    <os/>
5079                    <protocol>tcp</protocol>
5080                    <source>
5081                            <any/>
5082                    </source>
5083                    <destination>
5084                            <network>wanip</network>
5085                            <port>443</port>
5086                    </destination>
5087                    <descr><![CDATA[Allow to Port 443 on Firewall WAN]]></descr>
5088                    <updated>
5089                            <time>1493312279</time>
5090                            <username>admin@10.97.67.143</username>
5091                    </updated>
5092                    <created>
5093                            <time>1493312279</time>
5094                            <username>admin@10.97.67.143</username>
5095                    </created>
5096            </rule>
```

```
5097            <rule>
5098                    <id/>
5099                    <tracker>1493311302</tracker>
5100                    <type>pass</type>
5101                    <interface>wan</interface>
5102                    <ipprotocol>inet</ipprotocol>
5103                    <tag/>
5104                    <tagged/>
5105                    <max/>
5106                    <max-src-nodes/>
5107                    <max-src-conn/>
5108                    <max-src-states/>
5109                    <statetimeout/>
5110                    <statetype>keep state</statetype>
5111                    <os/>
5112                    <protocol>tcp</protocol>
5113                    <source>
5114                            <any/>
5115                    </source>
5116                    <destination>
5117                            <network>lan</network>
5118                            <port>3389</port>
5119                    </destination>
5120                    <descr><![CDATA[Allow RDP to LAN nodes]]></descr>
5121                    <updated>
5122                            <time>1493311302</time>
5123                            <username>admin@10.97.67.143</username>
5124                    </updated>
5125                    <created>
5126                            <time>1493311302</time>
5127                            <username>admin@10.97.67.143</username>
5128                    </created>
5129            </rule>
5130            <rule>
```

```
                <id/>
                <tracker>1469127156</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <disabled/>
                <descr/>
                <created>
                        <time>1469127156</time>
                        <username>admin@192.168.13.132</username>
                </created>
                <updated>
                        <time>1493311628</time>
                        <username>admin@10.97.67.143</username>
                </updated>
        </rule>
        <rule>
                <id/>
```

```
                        <tracker>1480964347</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <source>
                              <address>192.168.14.111</address>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                        <disabled/>
                        <descr><![CDATA[Allow Radiant (192.168.14.111) to Get Subnet 19
with]]></descr>
                        <created>
                              <time>1480964347</time>
                              <username>admin@10.97.67.144</username>
                        </created>
                        <updated>
                              <time>1493311596</time>
                              <username>admin@10.97.67.143</username>
                        </updated>
                  </rule>
                  <rule>
                        <id/>
                        <tracker>1480964466</tracker>
```

```
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <source>
                              <address>192.168.17.100</address>
                        </source>
                        <destination>
                              <any/>
                        </destination>
                        <disabled/>
                        <descr><![CDATA[Allow Radiant (192.168.17.100) to Get Subnet 19
from]]></descr>
                        <created>
                              <time>1480964466</time>
                              <username>admin@10.97.67.144</username>
                        </created>
                        <updated>
                              <time>1493311572</time>
                              <username>admin@10.97.67.143</username>
                        </updated>
                  </rule>
                  <rule>
                        <id/>
                        <tracker>1465935224</tracker>
                        <type>pass</type>
```

```
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>icmp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr/>
                <updated>
                        <time>1465935224</time>
                        <username>admin@192.168.18.100</username>
                </updated>
                <created>
                        <time>1465935224</time>
                        <username>admin@192.168.18.100</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1469127171</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
```

```
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <disabled/>
                <descr/>
                <created>
                        <time>1469127171</time>
                        <username>admin@192.168.13.132</username>
                </created>
                <updated>
                        <time>1493322054</time>
                        <username>admin@10.97.67.143</username>
                </updated>
        </rule>
        <rule>
                <id/>
                <tracker>1465935241</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
```

```
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>icmp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr/>
                <updated>
                        <time>1465935241</time>
                        <username>admin@192.168.18.100</username>
                </updated>
                <created>
                        <time>1465935241</time>
                        <username>admin@192.168.18.100</username>
                </created>
        </rule>
        <rule>
                <type>pass</type>
                <ipprotocol>inet</ipprotocol>
                <descr><![CDATA[Default allow LAN to any rule]]></descr>
                <interface>lan</interface>
                <tracker>0100000101</tracker>
                <source>
                        <network>lan</network>
                </source>
```

```
5335                    <destination>
5336                          <any/>
5337                    </destination>
5338              </rule>
5339              <rule>
5340                    <type>pass</type>
5341                    <ipprotocol>inet6</ipprotocol>
5342                    <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
5343                    <interface>lan</interface>
5344                    <tracker>0100000102</tracker>
5345                    <source>
5346                          <network>lan</network>
5347                    </source>
5348                    <destination>
5349                          <any/>
5350                    </destination>
5351              </rule>
5352              <separator>
5353                    <wan/>
5354                    <lan/>
5355                    <floatingrules/>
5356              </separator>
5357              <bypassstaticroutes>yes</bypassstaticroutes>
5358        </filter>
5359        <shaper>
5360        </shaper>
5361        <ipsec/>
5362        <aliases/>
5363        <proxyarp/>
5364        <cron>
5365              <item>
5366                    <minute>1,31</minute>
5367                    <hour>0-5</hour>
5368                    <mday>*</mday>
```

```
5369                    <month>*</month>
5370                    <wday>*</wday>
5371                    <who>root</who>
5372                    <command>/usr/bin/nice -n20 adjkerntz -a</command>
5373            </item>
5374            <item>
5375                    <minute>1</minute>
5376                    <hour>3</hour>
5377                    <mday>1</mday>
5378                    <month>*</month>
5379                    <wday>*</wday>
5380                    <who>root</who>
5381                    <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
5382            </item>
5383            <item>
5384                    <minute>*/60</minute>
5385                    <hour>*</hour>
5386                    <mday>*</mday>
5387                    <month>*</month>
5388                    <wday>*</wday>
5389                    <who>root</who>
5390                    <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
5391 sshlockout</command>
5392            </item>
5393            <item>
5394                    <minute>*/60</minute>
5395                    <hour>*</hour>
5396                    <mday>*</mday>
5397                    <month>*</month>
5398                    <wday>*</wday>
5399                    <who>root</who>
5400                    <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
5401 webConfiguratorlockout</command>
5402            </item>
5403            <item>
```

```
                        <minute>1</minute>
                        <hour>1</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
                </item>
                <item>
                        <minute>*/60</minute>
                        <hour>*</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
virusprot</command>
                </item>
                <item>
                        <minute>30</minute>
                        <hour>12</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
                </item>
        </cron>
        <wol/>
        <rrd>
                <enable/>
        </rrd>
        <load_balancer>
                <monitor_type>
```

```
5438                    <name>ICMP</name>
5439                    <type>icmp</type>
5440                    <descr><![CDATA[ICMP]]></descr>
5441                    <options/>
5442             </monitor_type>
5443             <monitor_type>
5444                    <name>TCP</name>
5445                    <type>tcp</type>
5446                    <descr><![CDATA[Generic TCP]]></descr>
5447                    <options/>
5448             </monitor_type>
5449             <monitor_type>
5450                    <name>HTTP</name>
5451                    <type>http</type>
5452                    <descr><![CDATA[Generic HTTP]]></descr>
5453                    <options>
5454                           <path>/</path>
5455                           <host/>
5456                           <code>200</code>
5457                    </options>
5458             </monitor_type>
5459             <monitor_type>
5460                    <name>HTTPS</name>
5461                    <type>https</type>
5462                    <descr><![CDATA[Generic HTTPS]]></descr>
5463                    <options>
5464                           <path>/</path>
5465                           <host/>
5466                           <code>200</code>
5467                    </options>
5468             </monitor_type>
5469             <monitor_type>
5470                    <name>SMTP</name>
5471                    <type>send</type>
```

```
                        <descr><![CDATA[Generic SMTP]]></descr>
                        <options>
                                <send/>
                                <expect>220 *</expect>
                        </options>
                </monitor_type>
        </load_balancer>
        <widgets>
        <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
/sequence>
        </widgets>
        <openvpn/>
        <dnshaper>
        </dnshaper>
        <unbound>
                <enable/>
                <dnssec/>
                <active_interface/>
                <outgoing_interface/>
                <custom_options/>
                <hideidentity/>
                <hideversion/>
                <dnssecstripped/>
        </unbound>
        <dhcpdv6>
                <lan>
                        <range>
                                <from>::1000</from>
                                <to>::2000</to>
                        </range>
                        <ramode>assist</ramode>
                        <rapriority>medium</rapriority>
                </lan>
        </dhcpdv6>
```

```
        <cert>
              <refid>5720a0502b277</refid>
              <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
              <type>server</type>

        <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXZ0F3SUJBZ0lCQURBTkJna3
Foa2lHOXcwQkFRc0ZBRENCdERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnTlZCQWdUQlZOMFlYUmxNUkV3RHdZ
RFZRUUhFd2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApaVzV6WlNCM1pXSkRiMjVtYVdkMWNtRjBiM0
lnVTJWc1ppMVRhV2R1WldRZ1EyVnlkR2xtYVdOaGRHVXhLREFtCkJna3Foa2lHOXcwQkNRRVdHV0ZrYldsdVFI
Qm1VMlZ1YzJVdWJHOWpZV3hrYjIxaGFXNHhIakFjQmdOVkJBTVQKRlhCbVUyVnVjMlV0TlRjeU1HRXdOVEF5WW
pJM056QWVGdzB4TmpBME1qY3hNVEU1TkRSYUZ3MHlNVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
d0pWVXpFT01Bd0dBMVVFQ0JNRlUzUmhkR1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNU1UZ3dOZ1lEVlFRS0
V5OXdabE5sYm5ObElZGxZa052Ym1acFozVnlZWFJ2Y2lCVFpXeG0KTFZOcFoyNWxaQ0JEWlhKMGFXWnBZMkYw
WlRFb01DWUdDU3FHU0liM0RRRUpBUllaWVdSdGFXNUFjR1pUWlc1egpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
dBMVVFQXhNVmNHWlRaVzV6WlMwMU56SXdZVEExTURKaU1qYzNNSUlCCklqQU5CZ2txaGtpRzl3MEJBUUVGQUFP
Q0FROEFNSUlCQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
hDODBHU0dhZnJENWdqcTRwZkNNMHlzbEFPaVlZK1hDYjdNa2o0dmtTMgpmbzl4emNyaDUrNVlaYlBHeXR1a2ls
ZWR4bjFWeFl6SllzYXZKdnlKb1lRMCtNTkx0dkFjYnRhTUFoZjh1ZkRFClhrclNVQ0N5YTFrbEYxNWJGZmcyUG
E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkUFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXd1SEZwd3J1LytYWExieEcrcD
dwYXI0aHR0UFRDcml1NmFqQVVTNmpvN05kOElQNWpzZ1kzR0h2ZjhzUUlECkFRQUJvNElCaGpDQ0FZSXdDUVlE
VlIwVEJBSXdBREFSQmdsZ2hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWkkKQVliNFFnRU5CQ1lXSkU5d1pXNV
RVMHdnUjJWdVpYSmhkR1ZrSUZObGNuWmxjaUJEWlhKMGFXWnBZMkYwWlRBZApCZ05WSFE0RUZnUVU3K1lLRmNp
OFFVSGhTZ0xEdjhFQ3NjQ0p3QUl3Z2VFR0ExVWRJd1NCMlRDQjFvQVU3K1lLCkZjaThRVUhoU2dMRHY4RUNzY0
NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsVlRNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
VUVCeE1JVEc5allXeHBkSGt4T0RBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaQpRMjl1Wm1sbmRYSmhkRzl5SU
ZObGJHWXRVMmxuYm1Wa0lFTmxjblJwWm1sallYUmxNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
bE5sYm5ObExteHZZMkZzZWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
56ZUNBUUF3SFFZRFZSMGxCQll3RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd0lG
b0RBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZFpQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmtNaTB5M0
9PWGtzWEs1cEM2dTd6Ukl3WjEvRjYyRUp3ODlUOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWJhRU42NEkxOHFud3Zm
S2JrREZvRThMR1hSdzBkMnAyTGVmYTd4YTIvSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG
c4bGdrcVc3dStlb01DNDJIbVJkOURCTmlzdFJ4RVlNMkFLQkFsZG1LYStvRUY1VUwwCm43aXpvNlZ4dHJWMTJv
TTdySllRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VVnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOVpPSmR2QmZLVU
1sUWlELyswSVpTalFXRDczWkdsaEhTK2tOeWc1aDJhUjUwYjh3Wm9zQnNjSUZDa0pFbgp0UT09Ci0tLS0tRU5E
IENFUlRJRklDQVRFLS0tLS0K</crt>

        <prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z0lCQURBTkJna3Foa2lHOXcwQkFRRU
ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M0lhYlkKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4
eGxiY3UyRUx6UVpJWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMWitqM0hOeXVIbjdsaGxzOG
JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcwdTI4Qnh1CjFvd0NGL3k1OE1SZVN0SlFJTEpyV1NVWFhs
c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcwdkEKQVdEQkQzNDg5OHRUalhROVNpb1NaclREbn
dKTmo3cHAwQnM4ZHhlRDBjL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
dHZFYjZudWxxdmlHMjA5TUt1SzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUpRRF
pxU3duMnNTUTh0SVNBTUVrUW0zcXhrb3BzdzB4cWNScmFlOEd4VmQKejBpOU1KbkZVQWFleTQvL3Jldndh ZW1P
R3RYSmZ2ai9jSnY3cmJIWGIzYkJtVW9hcDhxY0RjdnVSMmlHRUZYWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcD
lzNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1ZnlP
UzAvbXlmNU5YLzVoRklPNmFDc0xlUjZ4N1RZa2FDQU9FYlViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
hMZ0NRYlB2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUE0NzNMUWoxcExLSmRZN2JxCmtMU3NVT0ZhTUZlZG1xU2ttbzh3Qj
lpMXhzbElLQUd0M3U4dTdMZlZtU2lybnMwVVBTMHRVUDRyQXMzVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
OGttbFJnUFRmVHVPaGNwMGVkamQwK1E5Y2VlY25kaFp3UEl6TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHNhbm
NBRDhVYThDZ1lFQXpzYjYzbzRBSHlYNjZkcEJ6TGlzYzZxS2d2ZG4xazhVCm02N3RuK2M3NkVhSEtZTlk0Rjdh
S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUpOK0I3Sm
Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZm1DWlpRSUQ1OENnWUJjamFO
dk5obnFJOG9rWGhBUjR2c3NtNGpWb0tYU1ZScjRIVHo5MDFwOGdReXNCWkt0CnlUS2V6VThuUVZvTjNYWmVMbC
8rVEcwYVpKOTZHKy9nNTRWZmZqWTRlelVScHhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
```

```
QWY5Mi9CbHZJR25FS1pMdnhLWTdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
RG1hZGsvKy9Ud2UvVk1Kbmx2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUjlhbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBRS0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1Rlczdu
WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLClUzSThhYnpnUUtwOEwrZj
VadTAxY1pZVk5TU0FIUFRHYm5jb1IzbGVPYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>
```


```
        </cert>
        <revision>
                <time>1493327306</time>
                <description><![CDATA[admin@10.97.67.143: /firewall_rules_edit.php made
unknown change]]></description>
                <username>admin@10.97.67.143</username>
        </revision>
        <gateways>
                <gateway_item>
                        <interface>wan</interface>
                        <gateway>192.168.13.1</gateway>
                        <name>GW_WAN_2</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <interval/>
                        <descr><![CDATA[Interface wan Gateway]]></descr>
                </gateway_item>
                <gateway_item>
                        <interface>wan</interface>
                        <gateway>192.168.13.17</gateway>
                        <name>GW_VLAN17</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr><![CDATA[Gateway to VLAN 17]]></descr>
                </gateway_item>
        </gateways>
        <ppps/>
        <dyndnses/>
</pfSense>
```

2.10.3 Firewall Configuration for ID-ARM Subnet

```
<?xml version="1.0"?>
<pfSense>
	<version>15.4</version>
	<lastchange/>
	<theme>pfSense_ng</theme>
	<system>
		<optimization>normal</optimization>
		<hostname>FS-ARM</hostname>
		<domain>FS-ARM.gov</domain>
		<group>
			<name>all</name>
			<description><![CDATA[All Users]]></description>
			<scope>system</scope>
			<gid>1998</gid>
			<member>0</member>
		</group>
		<group>
			<name>admins</name>
			<description><![CDATA[System Administrators]]></description>
			<scope>system</scope>
			<gid>1999</gid>
			<member>0</member>
			<priv>page-all</priv>
		</group>
		<user>
			<name>admin</name>
			<descr><![CDATA[System Administrator]]></descr>
			<scope>system</scope>
			<groupname>admins</groupname>
			<password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
			<uid>0</uid>
			<priv>user-shell-access</priv>
		</user>
		<nextuid>2000</nextuid>
```

```
5635            <nextgid>2000</nextgid>
5636            <timezone>America/New_York</timezone>
5637            <time-update-interval/>
5638            <timeservers>10.97.74.8</timeservers>
5639            <webgui>
5640                  <protocol>http</protocol>
5641                  <loginautocomplete/>
5642                  <ssl-certref>5720a0502b277</ssl-certref>
5643                  <dashboardcolumns>2</dashboardcolumns>
5644                  <port/>
5645                  <max_procs>2</max_procs>
5646                  <nohttpreferercheck/>
5647            </webgui>
5648            <disablenatreflection>yes</disablenatreflection>
5649            <disablesegmentationoffloading/>
5650            <disablelargereceiveoffloading/>
5651            <ipv6allow/>
5652            <powerd_ac_mode>hadp</powerd_ac_mode>
5653            <powerd_battery_mode>hadp</powerd_battery_mode>
5654            <powerd_normal_mode>hadp</powerd_normal_mode>
5655            <bogons>
5656                  <interval>monthly</interval>
5657            </bogons>
5658            <language>en_US</language>
5659            <dns1gw>GW_WAN</dns1gw>
5660            <dns2gw>GW_WAN</dns2gw>
5661            <dns3gw>none</dns3gw>
5662            <dns4gw>none</dns4gw>
5663            <dnsserver>10.97.74.8</dnsserver>
5664            <dnsserver>10.63.255.2</dnsserver>
5665            <serialspeed>115200</serialspeed>
5666            <primaryconsole>serial</primaryconsole>
5667      </system>
5668      <interfaces>
```

```
5669                <wan>
5670                        <if>em0</if>
5671                        <descr><![CDATA[WAN]]></descr>
5672                        <enable/>
5673                        <spoofmac/>
5674                        <ipaddr>192.168.13.14</ipaddr>
5675                        <subnet>24</subnet>
5676                        <gateway>GW_WAN</gateway>
5677                </wan>
5678                <lan>
5679                        <enable/>
5680                        <if>em1</if>
5681                        <ipaddr>192.168.14.1</ipaddr>
5682                        <subnet>24</subnet>
5683                        <ipaddrv6/>
5684                        <subnetv6/>
5685                        <media/>
5686                        <mediaopt/>
5687                        <track6-interface>wan</track6-interface>
5688                        <track6-prefix-id>0</track6-prefix-id>
5689                        <gateway/>
5690                        <gatewayv6/>
5691                </lan>
5692        </interfaces>
5693        <staticroutes>
5694                <route>
5695                        <network>192.168.17.0/24</network>
5696                        <gateway>GW_VLAN17</gateway>
5697                        <descr><![CDATA[Route to VLAN 2017]]></descr>
5698                </route>
5699                <route>
5700                        <network>192.168.16.0/24</network>
5701                        <gateway>GW_VLAN16</gateway>
5702                        <descr><![CDATA[Route to VLAN 2016]]></descr>
```

```
5703                </route>
5704                <route>
5705                      <network>192.168.15.0/24</network>
5706                      <gateway>GW_VLAN15</gateway>
5707                      <descr><![CDATA[Route to VLAN 2015]]></descr>
5708                </route>
5709                <route>
5710                      <network>192.168.18.0/24</network>
5711                      <gateway>GW_VLAN18</gateway>
5712                      <descr><![CDATA[Route to VLAN 2018]]></descr>
5713                </route>
5714                <route>
5715                      <network>192.168.19.0/24</network>
5716                      <gateway>GW_VLAN19</gateway>
5717                      <descr><![CDATA[Route to VLAN 2019]]></descr>
5718                </route>
5719          </staticroutes>
5720          <dhcpd>
5721                <lan>
5722                      <enable/>
5723                      <range>
5724                            <from>192.168.14.100</from>
5725                            <to>192.168.14.150</to>
5726                      </range>
5727                </lan>
5728                <opt1>
5729                      <enable/>
5730                      <range>
5731                            <from>192.168.14.100</from>
5732                            <to>192.168.14.150</to>
5733                      </range>
5734                </opt1>
5735                <opt2>
5736                      <enable/>
```

```
                        <range>
                                <from>192.168.15.100</from>
                                <to>192.168.15.150</to>
                        </range>
                </opt2>
                <opt3>
                        <enable/>
                        <range>
                                <from>192.168.16.100</from>
                                <to>192.168.16.150</to>
                        </range>
                </opt3>
        </dhcpd>
        <snmpd>
                <syslocation/>
                <syscontact/>
                <rocommunity>public</rocommunity>
        </snmpd>
        <diag>
                <ipv6nat>
                        <ipaddr/>
                </ipv6nat>
        </diag>
        <bridge/>
        <syslog/>
        <nat>
                <outbound>
                        <mode>disabled</mode>
                </outbound>
        </nat>
        <filter>
                <rule>
                        <id/>
                        <tracker>1481037990</tracker>
```

```
5771                    <type>pass</type>
5772                    <interface>wan</interface>
5773                    <ipprotocol>inet</ipprotocol>
5774                    <tag/>
5775                    <tagged/>
5776                    <direction>any</direction>
5777                    <quick>yes</quick>
5778                    <floating>yes</floating>
5779                    <max/>
5780                    <max-src-nodes/>
5781                    <max-src-conn/>
5782                    <max-src-states/>
5783                    <statetimeout/>
5784                    <statetype>keep state</statetype>
5785                    <os/>
5786                    <protocol>tcp/udp</protocol>
5787                    <source>
5788                           <any/>
5789                    </source>
5790                    <destination>
5791                           <network>lan</network>
5792                           <port>3389</port>
5793                    </destination>
5794                    <descr><![CDATA[Allow RDP to LAN nodes]]></descr>
5795                    <created>
5796                           <time>1481037990</time>
5797                           <username>admin@10.97.67.155</username>
5798                    </created>
5799                    <updated>
5800                           <time>1493324042</time>
5801                           <username>admin@10.97.67.143</username>
5802                    </updated>
5803             </rule>
5804             <rule>
```

```
<id/>
<tracker>1481038086</tracker>
<type>pass</type>
<interface>wan</interface>
<ipprotocol>inet</ipprotocol>
<tag/>
<tagged/>
<direction>any</direction>
<quick>yes</quick>
<floating>yes</floating>
<max/>
<max-src-nodes/>
<max-src-conn/>
<max-src-states/>
<statetimeout/>
<statetype>keep state</statetype>
<os/>
<protocol>tcp/udp</protocol>
<source>
      <any/>
</source>
<destination>
      <network>lan</network>
      <port>2389</port>
</destination>
<descr><![CDATA[Allow Connection to Radiant Port 2389]]></descr>
<created>
      <time>1481038086</time>
      <username>admin@10.97.67.155</username>
</created>
<updated>
      <time>1493324258</time>
      <username>admin@10.97.67.143</username>
</updated>
```

```
5839            </rule>
5840            <rule>
5841                    <id/>
5842                    <tracker>1493650861</tracker>
5843                    <type>pass</type>
5844                    <interface>wan</interface>
5845                    <ipprotocol>inet</ipprotocol>
5846                    <tag/>
5847                    <tagged/>
5848                    <direction>any</direction>
5849                    <quick>yes</quick>
5850                    <floating>yes</floating>
5851                    <max/>
5852                    <max-src-nodes/>
5853                    <max-src-conn/>
5854                    <max-src-states/>
5855                    <statetimeout/>
5856                    <statetype>keep state</statetype>
5857                    <os/>
5858                    <protocol>tcp/udp</protocol>
5859                    <source>
5860                            <any/>
5861                    </source>
5862                    <destination>
5863                            <network>lan</network>
5864                            <port>389</port>
5865                    </destination>
5866                    <descr><![CDATA[Allow Connection to Port 389 in LAN]]></descr>
5867                    <updated>
5868                            <time>1493650861</time>
5869                            <username>admin@10.97.67.135</username>
5870                    </updated>
5871                    <created>
5872                            <time>1493650861</time>
```

```
                        <username>admin@10.97.67.135</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493650905</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os></os>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                        <port>636</port>
                </destination>
                <descr><![CDATA[Allow Connection to Port 636 in LAN]]></descr>
                <updated>
                        <time>1493650905</time>
                        <username>admin@10.97.67.135</username>
                </updated>
```

```
                        <created>
                                <time>1493650905</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1493328157</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp/udp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <network>lan</network>
                                <port>8089</port>
                        </destination>
                        <descr><![CDATA[Allow Connection to Radiant Port 8089]]></descr>
                        <updated>
                                <time>1493328157</time>
```

```
                        <username>admin@10.97.67.143</username>
                </updated>
                <created>
                        <time>1493328157</time>
                        <username>admin@10.97.67.143</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493328202</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                        <port>8090</port>
                </destination>
                <descr><![CDATA[Allow Connection to Radiant Port 8090]]></descr>
```

```
                        <updated>
                                <time>1493328202</time>
                                <username>admin@10.97.67.143</username>
                        </updated>
                        <created>
                                <time>1493328202</time>
                                <username>admin@10.97.67.143</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1493327695</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp/udp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <network>lan</network>
                                <port>8443</port>
```

```
6009                    </destination>
6010                    <descr><![CDATA[Allow Connection to Nextlabs port 8443]]></descr>
6011                    <updated>
6012                          <time>1493327695</time>
6013                          <username>admin@10.97.67.143</username>
6014                    </updated>
6015                    <created>
6016                          <time>1493327695</time>
6017                          <username>admin@10.97.67.143</username>
6018                    </created>
6019              </rule>
6020              <rule>
6021                    <id/>
6022                    <tracker>1493327739</tracker>
6023                    <type>pass</type>
6024                    <interface>wan</interface>
6025                    <ipprotocol>inet</ipprotocol>
6026                    <tag/>
6027                    <tagged/>
6028                    <direction>any</direction>
6029                    <quick>yes</quick>
6030                    <floating>yes</floating>
6031                    <max/>
6032                    <max-src-nodes/>
6033                    <max-src-conn/>
6034                    <max-src-states/>
6035                    <statetimeout/>
6036                    <statetype>keep state</statetype>
6037                    <os/>
6038                    <protocol>tcp</protocol>
6039                    <source>
6040                          <any/>
6041                    </source>
6042                    <destination>
```

```
                        <network>lan</network>
                        <port>443</port>
                </destination>
                <descr><![CDATA[Allow Connection to Nextlabs port 443]]></descr>
                <updated>
                        <time>1493327739</time>
                        <username>admin@10.97.67.143</username>
                </updated>
                <created>
                        <time>1493327739</time>
                        <username>admin@10.97.67.143</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493327782</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
```

```
6077                    </source>
6078                    <destination>
6079                          <any/>
6080                          <port>9233</port>
6081                    </destination>
6082                    <descr><![CDATA[Allow Connection to Nextlabs port 9233]]></descr>
6083                    <created>
6084                          <time>1493327782</time>
6085                          <username>admin@10.97.67.143</username>
6086                    </created>
6087                    <updated>
6088                          <time>1493327896</time>
6089                          <username>admin@10.97.67.143</username>
6090                    </updated>
6091              </rule>
6092              <rule>
6093                    <id/>
6094                    <tracker>1493327859</tracker>
6095                    <type>pass</type>
6096                    <interface>wan</interface>
6097                    <ipprotocol>inet</ipprotocol>
6098                    <tag/>
6099                    <tagged/>
6100                    <direction>any</direction>
6101                    <quick>yes</quick>
6102                    <floating>yes</floating>
6103                    <max/>
6104                    <max-src-nodes/>
6105                    <max-src-conn/>
6106                    <max-src-states/>
6107                    <statetimeout/>
6108                    <statetype>keep state</statetype>
6109                    <os/>
6110                    <protocol>tcp/udp</protocol>
```

```
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <any/>
                                <port>19888</port>
                        </destination>
                        <descr><![CDATA[Allow Connection to Nextlabs port 19888]]></descr>
                        <updated>
                                <time>1493327859</time>
                                <username>admin@10.97.67.143</username>
                        </updated>
                        <created>
                                <time>1493327859</time>
                                <username>admin@10.97.67.143</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1493325919</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
```

```
6145                    <os/>
6146                    <protocol>tcp/udp</protocol>
6147                    <source>
6148                           <network>lan</network>
6149                    </source>
6150                    <destination>
6151                           <any/>
6152                           <port>53</port>
6153                    </destination>
6154                    <descr><![CDATA[Allow DNS port 53 going out]]></descr>
6155                    <created>
6156                           <time>1493325919</time>
6157                           <username>admin@10.97.67.143</username>
6158                    </created>
6159                    <updated>
6160                           <time>1493326213</time>
6161                           <username>admin@10.97.67.143</username>
6162                    </updated>
6163             </rule>
6164             <rule>
6165                    <id/>
6166                    <tracker>1493328002</tracker>
6167                    <type>pass</type>
6168                    <ipprotocol>inet</ipprotocol>
6169                    <tag/>
6170                    <tagged/>
6171                    <direction>any</direction>
6172                    <quick>yes</quick>
6173                    <floating>yes</floating>
6174                    <max/>
6175                    <max-src-nodes/>
6176                    <max-src-conn/>
6177                    <max-src-states/>
6178                    <statetimeout/>
```

```
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                        <port>2000</port>
                </destination>
                <descr><![CDATA[Allow Connection to Nextlabs port 2000]]></descr>
                <updated>
                        <time>1493328002</time>
                        <username>admin@10.97.67.143</username>
                </updated>
                <created>
                        <time>1493328002</time>
                        <username>admin@10.97.67.143</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1481037313</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
```

```
                        <os/>
                        <source>
                                <address>192.168.14.111</address>
                        </source>
                        <destination>
                                <any/>
                        </destination>
                        <descr><![CDATA[Allow Radiant (192.168.14.111) to get out with any
p]]></descr>
                        <created>
                                <time>1481037313</time>
                                <username>admin@10.97.67.155</username>
                        </created>
                        <updated>
                                <time>1481037359</time>
                                <username>admin@10.97.67.155</username>
                        </updated>
                        <disabled/>
                </rule>
                <rule>
                        <id/>
                        <tracker>1480537443</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
```

```
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr><![CDATA[Allow Everything]]></descr>
                <updated>
                        <time>1480537443</time>
                        <username>admin@192.168.13.139</username>
                </updated>
                <created>
                        <time>1480537443</time>
                        <username>admin@192.168.13.139</username>
                </created>
                <disabled/>
        </rule>
        <rule>
                <id/>
                <tracker>1466105351</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>udp</protocol>
                <source>
```

```
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr/>
                <updated>
                        <time>1466105351</time>
                        <username>admin@192.168.13.101</username>
                </updated>
                <created>
                        <time>1466105351</time>
                        <username>admin@192.168.13.101</username>
                </created>
                <disabled/>
        </rule>
        <rule>
                <id/>
                <tracker>1465934980</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>icmp</protocol>
                <source>
                        <any/>
```

```
                </source>
                <destination>
                        <any/>
                </destination>
                <descr/>
                <updated>
                        <time>1465934980</time>
                        <username>admin@192.168.14.100</username>
                </updated>
                <created>
                        <time>1465934980</time>
                        <username>admin@192.168.14.100</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1461788221</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
```

```
                        <network>wanip</network>
                        <port>80</port>
                </destination>
                <descr><![CDATA[Allow to Port 80 on Firewall WAN]]></descr>
                <created>
                        <time>1461788221</time>
                        <username>admin@192.168.1.2</username>
                </created>
                <updated>
                        <time>1493323649</time>
                        <username>admin@10.97.67.143</username>
                </updated>
        </rule>
        <rule>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <descr><![CDATA[Easy Rule: Passed from Firewall Log
View]]></descr>
                <protocol>udp</protocol>
                <source>
                        <address>192.168.13.101</address>
                </source>
                <destination>
                        <address>192.168.13.102</address>
                        <port>137</port>
                </destination>
                <created>
                        <time>1466105470</time>
                        <username>Easy Rule</username>
                </created>
        </rule>
        <rule>
                <id/>
```

```
                <tracker>1480537570</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr><![CDATA[All Everything from LAN Interface]]></descr>
                <updated>
                        <time>1480537570</time>
                        <username>admin@192.168.13.139</username>
                </updated>
                <created>
                        <time>1480537570</time>
                        <username>admin@192.168.13.139</username>
                </created>
                <disabled/>
        </rule>
        <rule>
                <id/>
                <tracker>1466105363</tracker>
                <type>pass</type>
```

```
6417                    <interface>lan</interface>
6418                    <ipprotocol>inet</ipprotocol>
6419                    <tag/>
6420                    <tagged/>
6421                    <max/>
6422                    <max-src-nodes/>
6423                    <max-src-conn/>
6424                    <max-src-states/>
6425                    <statetimeout/>
6426                    <statetype>keep state</statetype>
6427                    <os/>
6428                    <protocol>udp</protocol>
6429                    <source>
6430                           <any/>
6431                    </source>
6432                    <destination>
6433                           <any/>
6434                    </destination>
6435                    <descr/>
6436                    <updated>
6437                           <time>1466105363</time>
6438                           <username>admin@192.168.13.101</username>
6439                    </updated>
6440                    <created>
6441                           <time>1466105363</time>
6442                           <username>admin@192.168.13.101</username>
6443                    </created>
6444                    <disabled/>
6445             </rule>
6446             <rule>
6447                    <id/>
6448                    <tracker>1465934995</tracker>
6449                    <type>pass</type>
6450                    <interface>lan</interface>
```

```
6451                    <ipprotocol>inet</ipprotocol>
6452                    <tag/>
6453                    <tagged/>
6454                    <max/>
6455                    <max-src-nodes/>
6456                    <max-src-conn/>
6457                    <max-src-states/>
6458                    <statetimeout/>
6459                    <statetype>keep state</statetype>
6460                    <os/>
6461                    <protocol>icmp</protocol>
6462                    <source>
6463                           <any/>
6464                    </source>
6465                    <destination>
6466                           <any/>
6467                    </destination>
6468                    <descr/>
6469                    <updated>
6470                           <time>1465934995</time>
6471                           <username>admin@192.168.14.100</username>
6472                    </updated>
6473                    <created>
6474                           <time>1465934995</time>
6475                           <username>admin@192.168.14.100</username>
6476                    </created>
6477             </rule>
6478             <rule>
6479                    <id/>
6480                    <tracker>1465915373</tracker>
6481                    <type>pass</type>
6482                    <interface>lan</interface>
6483                    <ipprotocol>inet</ipprotocol>
6484                    <tag/>
```

```
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr><![CDATA[Allow Any Any]]></descr>
                <updated>
                        <time>1465915373</time>
                        <username>admin@192.168.14.100</username>
                </updated>
                <created>
                        <time>1465915373</time>
                        <username>admin@192.168.14.100</username>
                </created>
                <disabled/>
        </rule>
        <rule>
                <type>pass</type>
                <ipprotocol>inet</ipprotocol>
                <descr><![CDATA[Default allow LAN to any rule]]></descr>
                <interface>lan</interface>
                <tracker>0100000101</tracker>
                <source>
                        <network>lan</network>
```

```
6519                    </source>
6520                    <destination>
6521                            <any/>
6522                    </destination>
6523            </rule>
6524            <rule>
6525                    <type>pass</type>
6526                    <ipprotocol>inet6</ipprotocol>
6527                    <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
6528                    <interface>lan</interface>
6529                    <tracker>0100000102</tracker>
6530                    <source>
6531                            <network>lan</network>
6532                    </source>
6533                    <destination>
6534                            <any/>
6535                    </destination>
6536            </rule>
6537            <separator>
6538                    <wan/>
6539                    <lan/>
6540                    <floatingrules/>
6541            </separator>
6542    </filter>
6543    <shaper>
6544    </shaper>
6545    <ipsec/>
6546    <aliases/>
6547    <proxyarp/>
6548    <cron>
6549            <item>
6550                    <minute>1,31</minute>
6551                    <hour>0-5</hour>
6552                    <mday>*</mday>
```

```
6553                    <month>*</month>
6554                    <wday>*</wday>
6555                    <who>root</who>
6556                    <command>/usr/bin/nice -n20 adjkerntz -a</command>
6557            </item>
6558            <item>
6559                    <minute>1</minute>
6560                    <hour>3</hour>
6561                    <mday>1</mday>
6562                    <month>*</month>
6563                    <wday>*</wday>
6564                    <who>root</who>
6565                    <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
6566            </item>
6567            <item>
6568                    <minute>*/60</minute>
6569                    <hour>*</hour>
6570                    <mday>*</mday>
6571                    <month>*</month>
6572                    <wday>*</wday>
6573                    <who>root</who>
6574                    <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
6575 sshlockout</command>
6576            </item>
6577            <item>
6578                    <minute>*/60</minute>
6579                    <hour>*</hour>
6580                    <mday>*</mday>
6581                    <month>*</month>
6582                    <wday>*</wday>
6583                    <who>root</who>
6584                    <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
6585 webConfiguratorlockout</command>
6586            </item>
6587            <item>
```

```
                        <minute>1</minute>
                        <hour>1</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
                </item>
                <item>
                        <minute>*/60</minute>
                        <hour>*</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
virusprot</command>
                </item>
                <item>
                        <minute>30</minute>
                        <hour>12</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
                </item>
        </cron>
        <wol/>
        <rrd>
                <enable/>
        </rrd>
        <load_balancer>
                <monitor_type>
```

```
6622                    <name>ICMP</name>
6623                    <type>icmp</type>
6624                    <descr><![CDATA[ICMP]]></descr>
6625                    <options/>
6626             </monitor_type>
6627             <monitor_type>
6628                    <name>TCP</name>
6629                    <type>tcp</type>
6630                    <descr><![CDATA[Generic TCP]]></descr>
6631                    <options/>
6632             </monitor_type>
6633             <monitor_type>
6634                    <name>HTTP</name>
6635                    <type>http</type>
6636                    <descr><![CDATA[Generic HTTP]]></descr>
6637                    <options>
6638                           <path>/</path>
6639                           <host/>
6640                           <code>200</code>
6641                    </options>
6642             </monitor_type>
6643             <monitor_type>
6644                    <name>HTTPS</name>
6645                    <type>https</type>
6646                    <descr><![CDATA[Generic HTTPS]]></descr>
6647                    <options>
6648                           <path>/</path>
6649                           <host/>
6650                           <code>200</code>
6651                    </options>
6652             </monitor_type>
6653             <monitor_type>
6654                    <name>SMTP</name>
6655                    <type>send</type>
```

```
                        <descr><![CDATA[Generic SMTP]]></descr>
                        <options>
                                <send/>
                                <expect>220 *</expect>
                        </options>
                </monitor_type>
        </load_balancer>
        <widgets>
        <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
/sequence>
        </widgets>
        <openvpn/>
        <dnshaper>
        </dnshaper>
        <unbound>
                <enable/>
                <dnssec/>
                <active_interface/>
                <outgoing_interface/>
                <custom_options/>
                <hideidentity/>
                <hideversion/>
                <dnssecstripped/>
        </unbound>
        <dhcpdv6>
                <lan>
                        <range>
                                <from>::1000</from>
                                <to>::2000</to>
                        </range>
                        <ramode>assist</ramode>
                        <rapriority>medium</rapriority>
                </lan>
        </dhcpdv6>
```

```
        <cert>
              <refid>5720a0502b277</refid>
              <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
              <type>server</type>

        <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXZ0F3SUJBZ0lCQURBTkJna3
Foa2lHOXcwQkFRc0ZBRENCdERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnTlZCQWdUQlZOMFlYUmxNUkV3RHdZ
RFZRUUhFd2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApaVzV6WlNCM1pXSkRiMjVtYVdkMWNtRjBiM0
lnVTJWc1ppMVRhV2R1WldRZ1EyVnlkR2xtYVdOaGRHVXhLREFtCkJna3Foa2lHOXcwQkNRRVdHV0ZrYldsdVFI
Qm1VMlZ1YzJVdWJHOWpZV3hrYjIxaGFXNHhIakFjQmdOVkJBTVQKRlhCbVUyVnVjMlV0TlRjeU1HRXdOVEF5WW
pJM056QWVGdzB4TmpBME1qY3hNVEU1TkRSYUZ3MHlNVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
d0pWVXpFT01Bd0dBMVVFQ0JNRlUzUmhkR1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNU1UZ3dOZ1lEVlFRS0
V5OXdabE5sYm5ObElIZGxZa052Ym1acFozVnlZWFJ2Y2lCVFpXeG0KTFZOcFoyNWxaQ0JEWlhKMGFXWnBZMkYw
WlRFb01DWUdDU3FHU0liM0RRRUpBUllaWVdSdGFXNUFjR1pUWlc1egpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
dBMVVFQXhNVmNHWlRaVzV6WlMwMU56SXdZVEExTURKaU1qYzNNSUlCCklqQU5CZ2txaGtpRzl3MEJBUUVGQUFP
Q0FROEFNSUlCQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
hDODBHU0dhZnJENWdqcTRwZkNNMHlzbEFPaVlZK1hDYjdNa2o0dmtTMgpmbzl4emNyaDUrNVlaYlBHeXR1a2ls
ZWR4bjFWeFl6SllzYXZKdnlKb1lRMCtNTkx0dkFjYnRhTUFoZjh1ZkRFClhrclNVQ0N5YTFrbEYxNWJGZmcyUG
E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkUFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXd1SEZwd3J1LytYWExieEcrcD
dwYXI0aHR0UFRDcml1NmFqQVVTNmpvN05kOElQNWpzZ1kzR0h2ZjhzUUlECkFRQUJvNElCaGpDQ0FZSXdDUVlE
VlIwVEJBSXdBREFSQmdsZ2hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWkkKQVliNFFnRU5CQ1lXSkU5d1pXNV
RVMHdnUjJWdVpYSmhkR1ZrSUZObGNuWmxjaUJEWlhKMGFXWnBZMkYwWlRBZApCZ05WSFE0RUZnUVU3K1lLRmNp
OFFVSGhTZ0xEdjhFQ3NjQ0p3QUl3Z2VFR0ExVWRJd1NCMlRDQjFvQVU3K1lLCkZjaThRVUhoU2dMRHY4RUNzY0
NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsVlRNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
VUVCeE1JVEc5allXeHBkSGt4T0RBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaQpRMjl1Wm1sbmRYSmhkRzl5SU
ZObGJHWXRVMmxuYm1Wa0lFTmxjblJwWm1sallYUmxNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
bE5sYm5ObExteHZZMkZzZWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
56ZUNBUUF3SFFZRFZSMGxCQll3RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd0lG
b0RBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZFpQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmtNaTB5M0
9PWGtzWEs1cEM2dTd6Ukl3WjEvRjYyRUp3ODlUOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWJhRU42NEkxOHFud3Zm
S2JrREZvRThMR1hSdzBkMnAyTGVmYTd4YTIvSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG
c4bGdrcVc3dStlb01DNDJIbVJkOURCTmlzdFJ4RVlNMkFLQkFsZG1LYStvRUY1VUwwCm43aXpvNlZ4dHJWMTJv
TTdySllRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VVnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOVpPSmR2QmZLVU
1sUWlELyswSVpTalFXRDczWkdsaEhTK2tOeWc1aDJhUjUwYjh3Wm9zQnNjSUZDa0pFbgp0UT09Ci0tLS0tRU5E
IENFUlRJRklDQVRFLS0tLS0K</crt>

        <prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z0lCQURBTkJna3Foa2lHOXcwQkFRRU
ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M0lhYlkKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4
eGxiY3UyRUx6UVpJWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMWitqM0hOeXVIbjdsaGxzOG
JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcwdTI4Qnh1CjFvd0NGL3k1OE1SZVN0SlFJTEpyV1NVWFhs
c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcwdkEKQVdEQkQzNDg5OHRUalhROVNpb1NaclREbn
dKTmo3cHAwQnM4ZHhlRDBjL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
dHZFYjZudWxxdmlHMjA5TUt1SzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUpRRF
pxU3duMnNTUTh0SVNBTUVrUW0zcXhrb3BzdzB4cWNScmFlOEd4VmQKejBpOU1KbkZVQWFleTQvL3Jldndh ZW1P
R3RYSmZ2ai9jSnY3cmJIWGIzYkJtVW9hcDhxY0RjdnVSMmlHRUZYWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcD
lzNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1ZnlP
UzAvbXlmNU5YLzVoRklPNmFDc0xlUjZ4N1RZa2FDQU9FYlViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
hMZ0NRYlB2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUE0NzNMUWoxcExLSmRZN2JxCmtMU3NVT0ZhTUZlZG1xU2ttbzh3Qj
lpMXhzbElLQUd0M3U4dTdMZlZtU2lybnMwVVBTMHRVUDRyQXMzVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
OGttbFJnUFRmVHVPaGNwMGVkamQwK1E5Y2VlY25kaFp3UEl6TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHNhbm
NBRDhVYThDZ1lFQXpzYjYzbzRBSHlYNjZkcEJ6TGlzYzZxS2d2ZG4xazhVCm02N3RuK2M3NkVhSEtZTlk0Rjdh
S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUpOK0I3Sm
Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZm1DWlpRSUQ1OENnWUJjamFO
dk5obnFJOG9rWGhBUjR2c3NtNGpWb0tYU1ZScjRIVHo5MDFwOGdReXNCWkt0CnlUS2V6VThuUVZvTjNYWmVMbC
8rVEcwYVpKOTZHKy9nNTRWZmZqWTRlelVScHhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
```

```
QWY5Mi9CbHZJR25FS1pMdnhLWTdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
RG1hZGsvKy9Ud2UvVk1Kbmx2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUjlhbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBRS0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1Rlczdu
WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLClUzSThhYnpnUUtwOEwrZj
VadTAxY1pZVk5TU0FIUFRHYm5jb1IzbGVPYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>
```


```
        </cert>
        <revision>
                <time>1493650905</time>
                <description><![CDATA[admin@10.97.67.135: /firewall_rules_edit.php made
unknown change]]></description>
                <username>admin@10.97.67.135</username>
        </revision>
        <gateways>
                <gateway_item>
                        <interface>lan</interface>
                        <gateway>dynamic</gateway>
                        <name>WAN_DHCP</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr><![CDATA[Interface WAN_DHCP Gateway]]></descr>
                </gateway_item>
                <gateway_item>
                        <interface>lan</interface>
                        <gateway>dynamic</gateway>
                        <name>WAN_DHCP</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr><![CDATA[Interface WAN_DHCP Gateway]]></descr>
                </gateway_item>
                <gateway_item>
                        <interface>lan</interface>
                        <gateway>dynamic</gateway>
                        <name>WAN_DHCP6</name>
                        <weight>1</weight>
                        <ipprotocol>inet6</ipprotocol>
```

```
6785                    <descr><![CDATA[Interface WAN_DHCP6 Gateway]]></descr>
6786                    <defaultgw/>
6787            </gateway_item>
6788            <gateway_item>
6789                    <interface>wan</interface>
6790                    <gateway>192.168.13.1</gateway>
6791                    <name>GW_WAN</name>
6792                    <weight>1</weight>
6793                    <ipprotocol>inet</ipprotocol>
6794                    <interval/>
6795                    <descr><![CDATA[Interface wan Gateway]]></descr>
6796                    <defaultgw/>
6797            </gateway_item>
6798            <gateway_item>
6799                    <interface>wan</interface>
6800                    <gateway>192.168.13.17</gateway>
6801                    <name>GW_VLAN17</name>
6802                    <weight>1</weight>
6803                    <ipprotocol>inet</ipprotocol>
6804                    <descr><![CDATA[Gateway to VLAN 17]]></descr>
6805            </gateway_item>
6806            <gateway_item>
6807                    <interface>wan</interface>
6808                    <gateway>192.168.13.16</gateway>
6809                    <name>GW_VLAN16</name>
6810                    <weight>1</weight>
6811                    <ipprotocol>inet</ipprotocol>
6812                    <descr><![CDATA[Gateway to VLAN 16]]></descr>
6813            </gateway_item>
6814            <gateway_item>
6815                    <interface>wan</interface>
6816                    <gateway>192.168.13.15</gateway>
6817                    <name>GW_VLAN15</name>
6818                    <weight>1</weight>
```

```
                        <ipprotocol>inet</ipprotocol>
                        <descr><![CDATA[Gateway to VLAN 15]]></descr>
                </gateway_item>
                <gateway_item>
                        <interface>wan</interface>
                        <gateway>192.168.13.18</gateway>
                        <name>GW_VLAN18</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr><![CDATA[Gateway to VLAN 18]]></descr>
                </gateway_item>
                <gateway_item>
                        <interface>wan</interface>
                        <gateway>192.168.13.19</gateway>
                        <name>GW_VLAN19</name>
                        <weight>1</weight>
                        <ipprotocol>inet</ipprotocol>
                        <descr><![CDATA[Gateway to VLAN 19]]></descr>
                </gateway_item>
        </gateways>
        <ppps/>
        <dyndnses/>
</pfSense>
```

2.10.4 Firewall Configuration for Private Cloud Subnet

```
<?xml version="1.0"?>
<pfSense>
        <version>15.4</version>
        <lastchange/>
        <theme>pfSense_ng</theme>
        <system>
                <optimization>normal</optimization>
                <hostname>FS-ARM</hostname>
                <domain>FS-ARM.gov</domain>
                <group>
```

```
6853                    <name>all</name>
6854                    <description><![CDATA[All Users]]></description>
6855                    <scope>system</scope>
6856                    <gid>1998</gid>
6857                    <member>0</member>
6858            </group>
6859            <group>
6860                    <name>admins</name>
6861                    <description><![CDATA[System Administrators]]></description>
6862                    <scope>system</scope>
6863                    <gid>1999</gid>
6864                    <member>0</member>
6865                    <priv>page-all</priv>
6866            </group>
6867            <user>
6868                    <name>admin</name>
6869                    <descr><![CDATA[System Administrator]]></descr>
6870                    <scope>system</scope>
6871                    <groupname>admins</groupname>
6872                    <password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
6873                    <uid>0</uid>
6874                    <priv>user-shell-access</priv>
6875            </user>
6876            <nextuid>2000</nextuid>
6877            <nextgid>2000</nextgid>
6878            <timezone>America/New_York</timezone>
6879            <time-update-interval/>
6880            <timeservers>10.97.74.8</timeservers>
6881            <webgui>
6882                    <protocol>http</protocol>
6883                    <loginautocomplete/>
6884                    <ssl-certref>5720a0502b277</ssl-certref>
6885                    <dashboardcolumns>2</dashboardcolumns>
6886                    <port/>
```

```
                        <max_procs>2</max_procs>
                        <nohttpreferercheck/>
                </webgui>
                <disablesegmentationoffloading/>
                <disablelargereceiveoffloading/>
                <ipv6allow/>
                <powerd_ac_mode>hadp</powerd_ac_mode>
                <powerd_battery_mode>hadp</powerd_battery_mode>
                <powerd_normal_mode>hadp</powerd_normal_mode>
                <bogons>
                        <interval>monthly</interval>
                </bogons>
                <language>en_US</language>
                <dns1gw>GW_WAN</dns1gw>
                <dns2gw>GW_WAN</dns2gw>
                <dns3gw>none</dns3gw>
                <dns4gw>none</dns4gw>
                <dnsserver>10.97.74.8</dnsserver>
                <dnsserver>10.63.255.2</dnsserver>
                <maximumstates/>
                <aliasesresolveinterval/>
                <maximumtableentries/>
                <maximumfrags/>
                <enablenatreflectionpurenat>yes</enablenatreflectionpurenat>
                <enablebinatreflection>yes</enablebinatreflection>
                <enablenatreflectionhelper>yes</enablenatreflectionhelper>
                <reflectiontimeout/>
                <serialspeed>115200</serialspeed>
                <primaryconsole>serial</primaryconsole>
        </system>
        <interfaces>
                <wan>
                        <if>em0</if>
                        <descr><![CDATA[WAN]]></descr>
```

```
                        <enable/>
                        <spoofmac/>
                        <ipaddr>192.168.13.20</ipaddr>
                        <subnet>24</subnet>
                        <gateway>GW_WAN_2</gateway>
                        <ipaddrv6/>
                        <subnetv6/>
                        <gatewayv6/>
                </wan>
                <lan>
                        <enable/>
                        <if>em1</if>
                        <ipaddr>192.168.20.1</ipaddr>
                        <subnet>24</subnet>
                        <ipaddrv6/>
                        <subnetv6/>
                        <media/>
                        <mediaopt/>
                        <track6-interface>wan</track6-interface>
                        <track6-prefix-id>0</track6-prefix-id>
                        <gateway/>
                        <gatewayv6/>
                </lan>
        </interfaces>
        <staticroutes/>
        <dhcpd>
                <lan>
                        <enable/>
                        <range>
                                <from>192.168.20.100</from>
                                <to>192.168.20.150</to>
                        </range>
                </lan>
                <opt1>
```

```
                        <enable/>
                        <range>
                                <from>192.168.14.100</from>
                                <to>192.168.14.150</to>
                        </range>
                </opt1>
                <opt2>
                        <enable/>
                        <range>
                                <from>192.168.15.100</from>
                                <to>192.168.15.150</to>
                        </range>
                </opt2>
                <opt3>
                        <enable/>
                        <range>
                                <from>192.168.16.100</from>
                                <to>192.168.16.150</to>
                        </range>
                </opt3>
        </dhcpd>
        <snmpd>
                <syslocation/>
                <syscontact/>
                <rocommunity>public</rocommunity>
        </snmpd>
        <diag>
                <ipv6nat>
                        <ipaddr/>
                </ipv6nat>
        </diag>
        <bridge/>
        <syslog/>
        <nat>
```

```
6989                <outbound>
6990                        <mode>automatic</mode>
6991                </outbound>
6992        </nat>
6993        <filter>
6994                <rule>
6995                        <id/>
6996                        <tracker>1493654453</tracker>
6997                        <type>pass</type>
6998                        <interface>wan</interface>
6999                        <ipprotocol>inet</ipprotocol>
7000                        <tag/>
7001                        <tagged/>
7002                        <direction>any</direction>
7003                        <quick>yes</quick>
7004                        <floating>yes</floating>
7005                        <max/>
7006                        <max-src-nodes/>
7007                        <max-src-conn/>
7008                        <max-src-states/>
7009                        <statetimeout/>
7010                        <statetype>keep state</statetype>
7011                        <os/>
7012                        <protocol>tcp</protocol>
7013                        <source>
7014                                <any/>
7015                        </source>
7016                        <destination>
7017                                <network>lan</network>
7018                                <port>443</port>
7019                        </destination>
7020                        <descr><![CDATA[Allow HTTPS connection to LAN server]]></descr>
7021                        <updated>
7022                                <time>1493654453</time>
```

```
                        <username>admin@10.97.67.135</username>
                </updated>
                <created>
                        <time>1493654453</time>
                        <username>admin@10.97.67.135</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493654529</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                        <port>80</port>
                </destination>
                <descr><![CDATA[Allow HTTP connection to LAN server]]></descr>
```

```
                        <updated>
                                <time>1493654529</time>
                                <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                                <time>1493654529</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1493654337</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <network>lan</network>
                                <port>3389</port>
```

```
                </destination>
                <descr><![CDATA[Allow RDP Connection to LAN servers]]></descr>
                <created>
                        <time>1493654337</time>
                        <username>admin@10.97.67.135</username>
                </created>
                <updated>
                        <time>1493654474</time>
                        <username>admin@10.97.67.135</username>
                </updated>
        </rule>
        <rule>
                <id/>
                <tracker>1469131237</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>wanip</network>
                        <port>80</port>
                </destination>
```

```
7125                    <descr><![CDATA[Allow Port 80 on WAN ]]></descr>
7126                    <created>
7127                           <time>1469131237</time>
7128                           <username>admin@192.168.20.103</username>
7129                    </created>
7130                    <updated>
7131                           <time>1493654100</time>
7132                           <username>admin@10.97.67.135</username>
7133                    </updated>
7134             </rule>
7135             <rule>
7136                    <id/>
7137                    <tracker>1465935224</tracker>
7138                    <type>pass</type>
7139                    <interface>wan</interface>
7140                    <ipprotocol>inet</ipprotocol>
7141                    <tag/>
7142                    <tagged/>
7143                    <max/>
7144                    <max-src-nodes/>
7145                    <max-src-conn/>
7146                    <max-src-states/>
7147                    <statetimeout/>
7148                    <statetype>keep state</statetype>
7149                    <os/>
7150                    <protocol>icmp</protocol>
7151                    <source>
7152                           <any/>
7153                    </source>
7154                    <destination>
7155                           <any/>
7156                    </destination>
7157                    <descr/>
7158                    <updated>
```

```
                        <time>1465935224</time>
                        <username>admin@192.168.18.100</username>
                </updated>
                <created>
                        <time>1465935224</time>
                        <username>admin@192.168.18.100</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1461788221</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>wanip</network>
                        <port>443</port>
                </destination>
                <descr><![CDATA[Allow Port 443 on WAN]]></descr>
                <created>
                        <time>1461788221</time>
```

```
                        <username>admin@192.168.1.2</username>
                </created>
                <updated>
                        <time>1493654159</time>
                        <username>admin@10.97.67.135</username>
                </updated>
        </rule>
        <rule>
                <id/>
                <tracker>1468437174</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr/>
                <updated>
                        <time>1468437174</time>
                        <username>admin@192.168.20.100</username>
                </updated>
```

```
                <created>
                        <time>1468437174</time>
                        <username>admin@192.168.20.100</username>
                </created>
                <disabled/>
        </rule>
        <rule>
                <id/>
                <tracker>1465935241</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>icmp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
                </destination>
                <descr/>
                <updated>
                        <time>1465935241</time>
                        <username>admin@192.168.18.100</username>
                </updated>
                <created>
```

```
                        <time>1465935241</time>
                        <username>admin@192.168.18.100</username>
                </created>
        </rule>
        <rule>
                <type>pass</type>
                <ipprotocol>inet</ipprotocol>
                <descr><![CDATA[Default allow LAN to any rule]]></descr>
                <interface>lan</interface>
                <tracker>0100000101</tracker>
                <source>
                        <network>lan</network>
                </source>
                <destination>
                        <any/>
                </destination>
        </rule>
        <rule>
                <type>pass</type>
                <ipprotocol>inet6</ipprotocol>
                <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
                <interface>lan</interface>
                <tracker>0100000102</tracker>
                <source>
                        <network>lan</network>
                </source>
                <destination>
                        <any/>
                </destination>
        </rule>
        <separator>
                <wan/>
                <lan/>
                <floatingrules/>
```

```
7295                </separator>
7296        </filter>
7297        <shaper>
7298        </shaper>
7299        <ipsec/>
7300        <aliases/>
7301        <proxyarp/>
7302        <cron>
7303                <item>
7304                        <minute>1,31</minute>
7305                        <hour>0-5</hour>
7306                        <mday>*</mday>
7307                        <month>*</month>
7308                        <wday>*</wday>
7309                        <who>root</who>
7310                        <command>/usr/bin/nice -n20 adjkerntz -a</command>
7311                </item>
7312                <item>
7313                        <minute>1</minute>
7314                        <hour>3</hour>
7315                        <mday>1</mday>
7316                        <month>*</month>
7317                        <wday>*</wday>
7318                        <who>root</who>
7319                        <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
7320                </item>
7321                <item>
7322                        <minute>*/60</minute>
7323                        <hour>*</hour>
7324                        <mday>*</mday>
7325                        <month>*</month>
7326                        <wday>*</wday>
7327                        <who>root</who>
```

```
                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
sshlockout</command>
                </item>
                <item>
                        <minute>*/60</minute>
                        <hour>*</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
webConfiguratorlockout</command>
                </item>
                <item>
                        <minute>1</minute>
                        <hour>1</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
                </item>
                <item>
                        <minute>*/60</minute>
                        <hour>*</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
virusprot</command>
                </item>
                <item>
                        <minute>30</minute>
                        <hour>12</hour>
```

```
                <mday>*</mday>
                <month>*</month>
                <wday>*</wday>
                <who>root</who>
                <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
        </item>
</cron>
<wol/>
<rrd>
        <enable/>
</rrd>
<load_balancer>
        <monitor_type>
                <name>ICMP</name>
                <type>icmp</type>
                <descr><![CDATA[ICMP]]></descr>
                <options/>
        </monitor_type>
        <monitor_type>
                <name>TCP</name>
                <type>tcp</type>
                <descr><![CDATA[Generic TCP]]></descr>
                <options/>
        </monitor_type>
        <monitor_type>
                <name>HTTP</name>
                <type>http</type>
                <descr><![CDATA[Generic HTTP]]></descr>
                <options>
                        <path>/</path>
                        <host/>
                        <code>200</code>
                </options>
        </monitor_type>
```

```
7397                <monitor_type>
7398                      <name>HTTPS</name>
7399                      <type>https</type>
7400                      <descr><![CDATA[Generic HTTPS]]></descr>
7401                      <options>
7402                            <path>/</path>
7403                            <host/>
7404                            <code>200</code>
7405                      </options>
7406                </monitor_type>
7407                <monitor_type>
7408                      <name>SMTP</name>
7409                      <type>send</type>
7410                      <descr><![CDATA[Generic SMTP]]></descr>
7411                      <options>
7412                            <send/>
7413                            <expect>220 *</expect>
7414                      </options>
7415                </monitor_type>
7416          </load_balancer>
7417          <widgets>
7418
7419          <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
7420    /sequence>
7421          </widgets>
7422          <openvpn/>
7423          <dnshaper>
7424          </dnshaper>
7425          <unbound>
7426                <dnssec/>
7427                <active_interface>all</active_interface>
7428                <outgoing_interface>all</outgoing_interface>
7429                <custom_options/>
7430                <hideidentity/>
7431                <hideversion/>
```

```
                <dnssecstripped/>
                <domainoverrides>
                        <domain>acmefinancial.com</domain>
                        <ip>192.168.19.10</ip>
                        <descr><![CDATA[Active Directory]]></descr>
                </domainoverrides>
                <port/>

        <system_domain_local_zone_type>transparent</system_domain_local_zone_type>
                <enable/>
        </unbound>
        <dhcpdv6>
                <lan>
                        <range>
                                <from>::1000</from>
                                <to>::2000</to>
                        </range>
                        <ramode>assist</ramode>
                        <rapriority>medium</rapriority>
                </lan>
        </dhcpdv6>
        <cert>
                <refid>5720a0502b277</refid>
                <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
                <type>server</type>

        <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXZ0F3SUJBZ0lCQURBTkJna3
Foa2lHOXcwQkFRc0ZBRENCdERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnTlZCQWdUQlZOMFlYUmxNUkV3RHdZ
RFZRUUhFd2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApaVzV6WlNCM1pXSkRiMjVtYVdkMWNtRjBiM0
lnVTJWc1ppMVRhV2R1WldRZ1EyVnlkR2xtYVdOaGRHVXhLREFtCkJna3Foa2lHOXcwQkNRRVdHV0ZrYldsdVFI
Qm1VMlZ1YzJVdWJHOWpZV3hrYjIxaGFXNHhIakFjQmdOVkJBTVQKRlhCbVUyVnVjMlV0TlRjeU1HRXdOVEF5WW
pJM056QWVGdzB4TmpBME1qY3hNVEU1TkRSYUZ3MHlNVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
d0pWVXpFT01Bd0dBMVVFQ0JNRlUzUmhkR1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNU1UZ3dOZ1lEVlFRS0
V5OXdabE5sYm5ObElIZGxZa052Ym1acFozVnlZWFJ2Y2lCVFpXeG0KTFZOcFoyNWxaQ0JEWlhKMGFXWnBZMkYw
WlRFb01DWUdDU3FHU0liM0RRRUpBUllaWVdSdGFXNUFjR1pUWlc1egpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
dBMVVFQXhNVmNHWlRaVzV6WlMwMU56SXdZVEExTURKaU1qYzNNSUlCCklqQU5CZ2txaGtpRzl3MEJBUUVGQUFP
Q0FROEFNSUlCQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
hDODBHU0dhZnJENWdqcTRwZkNNMHlzbEFPaVlZK1hDYjdNa2o0dmtTMgpmbzl4emNyaDUrNVlaYlBHeXR1a2ls
ZWR4bjFWeFl6SllzYXZKdnlKb1lRMCtNTkx0dkFjYnRhTUFoZjh1ZkRFClhrclNVQ0N5YTFrbEYxNWJGZmcyUG
E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkUFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXd1SEZwd3J1LytYWExieEcrcD
dwYXI0aHR0UFRDcml1NmFqQVVTNmpvN05kOElQNWpzZ1kzR0h2ZjhzUUlECkFRQUJvNElCaGpDQ0FZSXdDUVlE
VlIwVEJBSXdBREFSQmdsZ2hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWkkKQVliNFFnRU5CQ1lXSkU5d1pXNV
```

RVMHdnUjJWdVpYSmhkR1ZrSUZObGNuWmxjaUJEWlhKMGFXWnBZMkYwWlRBZApCZ05WSFE0RUZnUVU3K1lLRmNp
OFFVSGhTZ0xEdjhFQ3NjQ0p3QUl3Z2VFR0ExVWRJd1NCMlRDQjFvQVU3K1lLCkZjaThRVUhoU2dMRHY4RUNzY0
NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsVlRNUTR3REFZRFZRUUkRXdWVGRHRjBaVEVSTUE4R0Ex
VUVCeE1JVEc5allXeHBkSGt4T0RBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaQpRMjl1Wm1sbmRYSmhkRzl5SU
ZObGJHWXRVMmxuYm1Wa0lFTmxjblJwWm1sallYUmxNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
bE5sYm5ObExteHZZMkZzWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
56ZUNBUUF3SFFZRFZSMGxCQll3RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd0lG
b0RBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZFpQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmtNaTB5M0
9PWGtzWEs1cEM2dTd6Ukl3WjEvRjYyRUp3ODlUOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWJhRU42NEkxOHFud3Zm
S2JrREZvRThMR1hSdzBkMnAyTGVmYTd4YTIvSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG
c4bGdrcVc3dStlb01DNDJIbVJkOURCTmlzdFJ4RVlNMkFLQkFsZG1LYStvRUY1VUwwCm43aXpvNlZ4dHJWMTJv
TTdySllRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VVnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOVpPSmR2QmZLVU
1sUWlELyswSVpTalFXRDczWkdsaEhTK2tOeWc1aDJhUjUwYjh3Wm9zQnNjSUZDa0pFbgp0UT09Ci0tLS0tRU5E
IENFUlRJRklDQVRFLS0tLS0K</crt>

<prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z0lCQURBTkJna3Foa2lHOXcwQkFRRU
ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M0lhYlkKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4
eGxiY3UyRUx6UVpJWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMWitqM0hOeXVIbjdsaGxzOG
JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcwdTI4Qnh1CjFvd0NGL3k1OE1SZVN0SlFJTEpyV1NVWFhs
c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcwdkEKQVdEQkQzNDg5OHRUalhROVNpb1NaclREEbn
dKTmo3cHAwQnM4ZHhlRDBjL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
dHZFYjZudWxxdmlHMjA5TUt1SzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUpRRF
pxU3duMnNTUTh0SVNBTUVrUW0zcXhrb3BzdzB4cWNScmFlOEd4VmQKejBpOU1KbkZVQWFleTQvL3Jldndh ZW1P
R3RYSmZ2ai9jSnY3cmJIWGIzYkJtVW9hcDhxY0RjdnVSMmlHRUZYWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcD
lzNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1ZnlP
UzAvbXlmNU5YLzVoRklPNmFDc0xlUjZ4N1RZa2FDQU9FYlViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
hMZ0NRYlB2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUE0NzNMUWoxcExLSmRZN2JxCmtMU3NVT0ZhTUZlZG1xU2ttbzh3Qj
lpMXhzbElLQUd0M3U4dTdMZlZtU2lybnMwVVBTMHRVUDRyQXMzVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
OGttbFJnUFRmVHVPaGNwMGVkamQwK1E5Y2VlY25kaFp3UEl6TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHNhbm
NBRDhVYThDZ1lFQXpzYjYzbzRBSHlYNjZkcEJ6TGlzYzZxS2d2ZG4xazhVCm02N3RuK2M3NkVhSEtZTlk0Rjdh
S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUpOK0I3Sm
Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZm1DWlpRSUQ1OENnWUJjamFO
dk5obnFJOG9rWGhBUjR2c3NtNGpWb0tYU1ZScjRIVHo5MDFwOGdReXNCWkt0CnlUS2V6VThuUVZvTjNYWmVMbC
8rVEcwYVpKOTZHKy9nNTRWZmZqWTRlelVScHhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
QWY5Mi9CbHZJR25FS1pMdnhLWTdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
RG1hZGsvKy9Ud2UvVk1Kbmx2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUjlhbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBRS0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1Rlczdu
WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLClUzSThhYnpnUUtwOEwrZj
VadTAxY1pZVk5TU0FIUFRHYm5jb1IzbGVPYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>

</cert>

<revision>

<time>1493654529</time>

<description><![CDATA[admin@10.97.67.135: /firewall_rules_edit.php made unknown change]]></description>

<username>admin@10.97.67.135</username>

</revision>

<gateways>

<gateway_item>

<interface>wan</interface>

```
                    <gateway>192.168.13.1</gateway>
                    <name>GW_WAN_2</name>
                    <weight>1</weight>
                    <ipprotocol>inet</ipprotocol>
                    <interval/>
                    <descr><![CDATA[Interface wan Gateway]]></descr>
              </gateway_item>
       </gateways>
       <ppps/>
       <dyndnses/>
       <dnsmasq>
              <enable/>
              <custom_options/>
              <port>53</port>
              <interface/>
              <hosts>
                    <host>activedirectory</host>
                    <domain>acmefinancial.com</domain>
                    <ip>192.168.19.10</ip>
                    <descr/>
                    <aliases/>
              </hosts>
       </dnsmasq>
</pfSense>
```

2.10.5 Firewall Configuration for the Management and Monitoring Subnet

```
<?xml version="1.0"?>
<pfSense>
       <version>15.4</version>
       <lastchange/>
       <theme>pfSense_ng</theme>
       <system>
              <optimization>normal</optimization>
              <hostname>FS-ARM</hostname>
              <domain>FS-ARM.gov</domain>
```

```
7561            <group>
7562                    <name>all</name>
7563                    <description><![CDATA[All Users]]></description>
7564                    <scope>system</scope>
7565                    <gid>1998</gid>
7566                    <member>0</member>
7567            </group>
7568            <group>
7569                    <name>admins</name>
7570                    <description><![CDATA[System Administrators]]></description>
7571                    <scope>system</scope>
7572                    <gid>1999</gid>
7573                    <member>0</member>
7574                    <priv>page-all</priv>
7575            </group>
7576            <user>
7577                    <name>admin</name>
7578                    <descr><![CDATA[System Administrator]]></descr>
7579                    <scope>system</scope>
7580                    <groupname>admins</groupname>
7581                    <password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
7582                    <uid>0</uid>
7583                    <priv>user-shell-access</priv>
7584            </user>
7585            <nextuid>2000</nextuid>
7586            <nextgid>2000</nextgid>
7587            <timezone>America/New_York</timezone>
7588            <time-update-interval/>
7589            <timeservers>10.97.74.8</timeservers>
7590            <webgui>
7591                    <protocol>http</protocol>
7592                    <loginautocomplete/>
7593                    <ssl-certref>5720a0502b277</ssl-certref>
7594                    <dashboardcolumns>2</dashboardcolumns>
```

```
                        <port/>
                        <max_procs>2</max_procs>
                        <nohttpreferercheck/>
                </webgui>
                <disablenatreflection>yes</disablenatreflection>
                <disablesegmentationoffloading/>
                <disablelargereceiveoffloading/>
                <ipv6allow/>
                <powerd_ac_mode>hadp</powerd_ac_mode>
                <powerd_battery_mode>hadp</powerd_battery_mode>
                <powerd_normal_mode>hadp</powerd_normal_mode>
                <bogons>
                        <interval>monthly</interval>
                </bogons>
                <language>en_US</language>
                <dns1gw>GW_WAN</dns1gw>
                <dns2gw>GW_WAN</dns2gw>
                <dns3gw>none</dns3gw>
                <dns4gw>none</dns4gw>
                <dnsserver>10.97.74.8</dnsserver>
                <dnsserver>10.63.255.2</dnsserver>
                <serialspeed>115200</serialspeed>
                <primaryconsole>serial</primaryconsole>
                <maximumstates/>
                <aliasesresolveinterval/>
                <maximumtableentries/>
                <maximumfrags/>
                <reflectiontimeout/>
        </system>
        <interfaces>
                <wan>
                        <if>em0</if>
                        <descr><![CDATA[WAN]]></descr>
                        <enable/>
```

```
                    <spoofmac/>
                    <ipaddr>192.168.13.17</ipaddr>
                    <subnet>24</subnet>
                    <gateway>GW_WAN_2</gateway>
                    <ipaddrv6/>
                    <subnetv6/>
                    <gatewayv6/>
             </wan>
             <lan>
                    <enable/>
                    <if>em1</if>
                    <ipaddr>192.168.17.1</ipaddr>
                    <subnet>24</subnet>
                    <ipaddrv6/>
                    <subnetv6/>
                    <media/>
                    <mediaopt/>
                    <track6-interface>wan</track6-interface>
                    <track6-prefix-id>0</track6-prefix-id>
                    <gateway/>
                    <gatewayv6/>
             </lan>
      </interfaces>
      <staticroutes>
             <route>
                    <network>192.168.19.0/24</network>
                    <gateway>GW_VLAN19</gateway>
                    <descr><![CDATA[Route to VLAN 2019]]></descr>
             </route>
      </staticroutes>
      <dhcpd>
             <lan>
                    <enable/>
                    <range>
```

```
                        <from>192.168.17.100</from>
                        <to>192.168.17.150</to>
                    </range>
                </lan>
                <opt1>
                    <enable/>
                    <range>
                        <from>192.168.14.100</from>
                        <to>192.168.14.150</to>
                    </range>
                </opt1>
                <opt2>
                    <enable/>
                    <range>
                        <from>192.168.15.100</from>
                        <to>192.168.15.150</to>
                    </range>
                </opt2>
                <opt3>
                    <enable/>
                    <range>
                        <from>192.168.16.100</from>
                        <to>192.168.16.150</to>
                    </range>
                </opt3>
        </dhcpd>
        <snmpd>
                <syslocation/>
                <syscontact/>
                <rocommunity>public</rocommunity>
        </snmpd>
        <diag>
                <ipv6nat>
                    <ipaddr/>
```

```
7697                </ipv6nat>
7698          </diag>
7699          <bridge/>
7700          <syslog/>
7701          <nat>
7702                <outbound>
7703                      <mode>disabled</mode>
7704                </outbound>
7705                <rule>
7706                      <source>
7707                            <any/>
7708                      </source>
7709                      <destination>
7710                            <address>192.168.13.171</address>
7711                            <port>5176</port>
7712                      </destination>
7713                      <protocol>tcp/udp</protocol>
7714                      <target>192.168.17.11</target>
7715                      <local-port>5176</local-port>
7716                      <interface>wan</interface>
7717                      <descr><![CDATA[Mapping to ConsoleWorks]]></descr>
7718                      <associated-rule-id>nat_57bf06b1aa4c21.26556306</associated-rule-
7719    id>
7720                      <natreflection>purenat</natreflection>
7721                      <created>
7722                            <time>1472136881</time>
7723                            <username>admin@192.168.13.135</username>
7724                      </created>
7725                      <updated>
7726                            <time>1472137126</time>
7727                            <username>admin@192.168.13.135</username>
7728                      </updated>
7729                </rule>
7730                <separator/>
```

```
        </nat>
        <filter>
                <rule>
                        <id/>
                        <tracker>1493655499</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os></os>
                        <protocol>tcp/udp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <network>lan</network>
                                <port>514</port>
                        </destination>
                        <descr><![CDATA[Allow Connection to syslog in LAN]]></descr>
                        <updated>
                                <time>1493655499</time>
                                <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
```

```
                        <time>1493655499</time>
                        <username>admin@10.97.67.135</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493649494</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                        <port>1433-1434</port>
                </destination>
                <descr><![CDATA[Allow Connection to Sharepoint database-1433 and
143]]></descr>
                <created>
                        <time>1493649494</time>
```

```
7799                        <username>admin@10.97.67.135</username>
7800                  </created>
7801                  <updated>
7802                        <time>1493649550</time>
7803                        <username>admin@10.97.67.135</username>
7804                  </updated>
7805            </rule>
7806            <rule>
7807                  <id/>
7808                  <tracker>1493649686</tracker>
7809                  <type>pass</type>
7810                  <interface>wan</interface>
7811                  <ipprotocol>inet</ipprotocol>
7812                  <tag/>
7813                  <tagged/>
7814                  <direction>any</direction>
7815                  <quick>yes</quick>
7816                  <floating>yes</floating>
7817                  <max/>
7818                  <max-src-nodes/>
7819                  <max-src-conn/>
7820                  <max-src-states/>
7821                  <statetimeout/>
7822                  <statetype>keep state</statetype>
7823                  <os/>
7824                  <protocol>tcp</protocol>
7825                  <source>
7826                        <any/>
7827                  </source>
7828                  <destination>
7829                        <network>lan</network>
7830                        <port>3389</port>
7831                  </destination>
7832                  <descr><![CDATA[Allow Connection to RDP in LAN]]></descr>
```

```
                        <updated>
                                <time>1493649686</time>
                                <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                                <time>1493649686</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1493649754</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <network>lan</network>
                                <port>389</port>
```

```
                </destination>
                <descr><![CDATA[Allow LDAP Connection to LAN]]></descr>
                <created>
                        <time>1493649754</time>
                        <username>admin@10.97.67.135</username>
                </created>
                <updated>
                        <time>1493650257</time>
                        <username>admin@10.97.67.135</username>
                </updated>
        </rule>
        <rule>
                <id/>
                <tracker>1493650231</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
```

```
                        <network>lan</network>
                        <port>2389</port>
                </destination>
                <descr><![CDATA[Allow Alternate LDAP Connection to Radiant
]]></descr>
                <updated>
                        <time>1493650231</time>
                        <username>admin@10.97.67.135</username>
                </updated>
                <created>
                        <time>1493650231</time>
                        <username>admin@10.97.67.135</username>
                </created>
        </rule>
        <rule>
                <id/>
                <tracker>1493649801</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp</protocol>
                <source>
```

```
                        <any/>
                </source>
                <destination>
                        <network>lan</network>
                        <port>636</port>
                </destination>
                <descr><![CDATA[Allow LDAPS Connection to LAN]]></descr>
                <created>
                        <time>1493649801</time>
                        <username>admin@10.97.67.135</username>
                </created>
                <updated>
                        <time>1493650283</time>
                        <username>admin@10.97.67.135</username>
                </updated>
        </rule>
        <rule>
                <id/>
                <tracker>1493649895</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <direction>any</direction>
                <quick>yes</quick>
                <floating>yes</floating>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
```

```
                        <protocol>tcp</protocol>
                        <source>
                                <any/>
                        </source>
                        <destination>
                                <network>lan</network>
                                <port>8000</port>
                        </destination>
                        <descr><![CDATA[Allow Connection to Port 8000 -Splunk
Web]]></descr>
                        <created>
                                <time>1493649895</time>
                                <username>admin@10.97.67.135</username>
                        </created>
                        <updated>
                                <time>1493649933</time>
                                <username>admin@10.97.67.135</username>
                        </updated>
                </rule>
                <rule>
                        <id/>
                        <tracker>1493650131</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
```

```
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp</protocol>
                        <source>
                              <any/>
                        </source>
                        <destination>
                              <network>lan</network>
                              <port>8089</port>
                        </destination>
                        <descr><![CDATA[Allow Connection to Port 8089 -Splunk management
por]]></descr>
                        <updated>
                              <time>1493650131</time>
                              <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                              <time>1493650131</time>
                              <username>admin@10.97.67.135</username>
                        </created>
                  </rule>
                  <rule>
                        <id/>
                        <tracker>1493650643</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
```

```
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp</protocol>
                        <source>
                               <any/>
                        </source>
                        <destination>
                               <network>lan</network>
                               <port>9997</port>
                        </destination>
                        <descr><![CDATA[Allow Connection to Port 9997 -Splunk
Forwarding]]></descr>
                        <updated>
                               <time>1493650643</time>
                               <username>admin@10.97.67.135</username>
                        </updated>
                        <created>
                               <time>1493650643</time>
                               <username>admin@10.97.67.135</username>
                        </created>
                </rule>
                <rule>
                        <id/>
                        <tracker>1481037634</tracker>
                        <type>pass</type>
                        <interface>lan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
                        <tagged/>
                        <direction>any</direction>
```

```
                        <quick>yes</quick>
                        <floating>yes</floating>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <source>
                                <address>192.168.17.100</address>
                        </source>
                        <destination>
                                <any/>
                        </destination>
                        <descr><![CDATA[Allow Radiant (192.168.17.100) to outside -
LAN]]></descr>
                        <created>
                                <time>1481037634</time>
                                <username>admin@10.97.67.155</username>
                        </created>
                        <updated>
                                <time>1481037861</time>
                                <username>admin@10.97.67.155</username>
                        </updated>
                        <disabled/>
                </rule>
                <rule>
                        <id/>
                        <tracker>1481037754</tracker>
                        <type>pass</type>
                        <interface>wan</interface>
                        <ipprotocol>inet</ipprotocol>
                        <tag/>
```

```
8105                    <tagged/>
8106                    <direction>any</direction>
8107                    <quick>yes</quick>
8108                    <floating>yes</floating>
8109                    <max/>
8110                    <max-src-nodes/>
8111                    <max-src-conn/>
8112                    <max-src-states/>
8113                    <statetimeout/>
8114                    <statetype>keep state</statetype>
8115                    <os/>
8116                    <source>
8117                           <address>192.168.17.100</address>
8118                    </source>
8119                    <destination>
8120                           <any/>
8121                    </destination>
8122                    <descr><![CDATA[Allow Radiant (192.168.17.100) to outside -
8123 WAN]]></descr>
8124                    <created>
8125                           <time>1481037754</time>
8126                           <username>admin@10.97.67.155</username>
8127                    </created>
8128                    <updated>
8129                           <time>1481037814</time>
8130                           <username>admin@10.97.67.155</username>
8131                    </updated>
8132                    <disabled/>
8133             </rule>
8134             <rule>
8135                    <id/>
8136                    <tracker>1472179706</tracker>
8137                    <type>pass</type>
8138                    <interface>wan,lan</interface>
```

```
8139                    <ipprotocol>inet</ipprotocol>
8140                    <tag/>
8141                    <tagged/>
8142                    <direction>any</direction>
8143                    <quick>yes</quick>
8144                    <floating>yes</floating>
8145                    <max/>
8146                    <max-src-nodes/>
8147                    <max-src-conn/>
8148                    <max-src-states/>
8149                    <statetimeout/>
8150                    <statetype>keep state</statetype>
8151                    <os/>
8152                    <protocol>tcp</protocol>
8153                    <source>
8154                          <any/>
8155                    </source>
8156                    <destination>
8157                          <any/>
8158                    </destination>
8159                    <descr><![CDATA[Test for comms between 2017 and 2019]]></descr>
8160                    <updated>
8161                          <time>1472179706</time>
8162                          <username>admin@10.97.67.137</username>
8163                    </updated>
8164                    <created>
8165                          <time>1472179706</time>
8166                          <username>admin@10.97.67.137</username>
8167                    </created>
8168                    <disabled/>
8169              </rule>
8170              <rule>
8171                    <id/>
8172                    <tracker>1469130242</tracker>
```

```
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <network>wanip</network>
                        <port>80</port>
                </destination>
                <descr><![CDATA[Allow to Port 80 on Firewall WAN]]></descr>
                <created>
                        <time>1469130242</time>
                        <username>admin@192.168.17.103</username>
                </created>
                <updated>
                        <time>1493649052</time>
                        <username>admin@10.97.67.135</username>
                </updated>
        </rule>
        <rule>
                <id/>
                <tracker>1465935549</tracker>
                <type>pass</type>
```

```
8207                    <interface>wan</interface>
8208                    <ipprotocol>inet</ipprotocol>
8209                    <tag/>
8210                    <tagged/>
8211                    <max/>
8212                    <max-src-nodes/>
8213                    <max-src-conn/>
8214                    <max-src-states/>
8215                    <statetimeout/>
8216                    <statetype>keep state</statetype>
8217                    <os/>
8218                    <protocol>icmp</protocol>
8219                    <source>
8220                           <any/>
8221                    </source>
8222                    <destination>
8223                           <any/>
8224                    </destination>
8225                    <descr/>
8226                    <updated>
8227                           <time>1465935549</time>
8228                           <username>admin@192.168.17.100</username>
8229                    </updated>
8230                    <created>
8231                           <time>1465935549</time>
8232                           <username>admin@192.168.17.100</username>
8233                    </created>
8234             </rule>
8235             <rule>
8236                    <id/>
8237                    <tracker>1461788221</tracker>
8238                    <type>pass</type>
8239                    <interface>wan</interface>
8240                    <ipprotocol>inet</ipprotocol>
```

```
                        <tag/>
                        <tagged/>
                        <max/>
                        <max-src-nodes/>
                        <max-src-conn/>
                        <max-src-states/>
                        <statetimeout/>
                        <statetype>keep state</statetype>
                        <os/>
                        <protocol>tcp</protocol>
                        <source>
                              <any/>
                        </source>
                        <destination>
                              <network>wanip</network>
                              <port>443</port>
                        </destination>
                        <descr><![CDATA[Allow to Port 443 on Firewall WAN]]></descr>
                        <created>
                              <time>1461788221</time>
                              <username>admin@192.168.1.2</username>
                        </created>
                        <updated>
                              <time>1493649121</time>
                              <username>admin@10.97.67.135</username>
                        </updated>
                  </rule>
                  <rule>
                        <source>
                              <any/>
                        </source>
                        <interface>wan</interface>
                        <protocol>tcp/udp</protocol>
                        <destination>
```

```
                        <address>192.168.17.11</address>
                        <port>5176</port>
                </destination>
                <descr><![CDATA[NAT Mapping to ConsoleWorks]]></descr>
                <associated-rule-id>nat_57bf06b1aa4c21.26556306</associated-rule-
id>
                <tracker>1472136881</tracker>
                <created>
                        <time>1472136881</time>
                        <username>NAT Port Forward</username>
                </created>
                <disabled/>
        </rule>
        <rule>
                <id/>
                <tracker>1469130278</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>tcp/udp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
```

```
                        <port>22</port>
                </destination>
                <descr><![CDATA[Test to port 22]]></descr>
                <created>
                        <time>1469130278</time>
                        <username>admin@192.168.17.103</username>
                </created>
                <updated>
                        <time>1472170372</time>
                        <username>admin@192.168.13.135</username>
                </updated>
                <disabled/>
        </rule>
        <rule>
                <id/>
                <tracker>1465935564</tracker>
                <type>pass</type>
                <interface>lan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag/>
                <tagged/>
                <max/>
                <max-src-nodes/>
                <max-src-conn/>
                <max-src-states/>
                <statetimeout/>
                <statetype>keep state</statetype>
                <os/>
                <protocol>icmp</protocol>
                <source>
                        <any/>
                </source>
                <destination>
                        <any/>
```

```
                </destination>
                <descr/>
                <updated>
                        <time>1465935564</time>
                        <username>admin@192.168.17.100</username>
                </updated>
                <created>
                        <time>1465935564</time>
                        <username>admin@192.168.17.100</username>
                </created>
        </rule>
        <rule>
                <type>pass</type>
                <ipprotocol>inet</ipprotocol>
                <descr><![CDATA[Default allow LAN to any rule]]></descr>
                <interface>lan</interface>
                <tracker>0100000101</tracker>
                <source>
                        <network>lan</network>
                </source>
                <destination>
                        <any/>
                </destination>
        </rule>
        <rule>
                <type>pass</type>
                <ipprotocol>inet6</ipprotocol>
                <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
                <interface>lan</interface>
                <tracker>0100000102</tracker>
                <source>
                        <network>lan</network>
                </source>
                <destination>
```

```
                        <any/>
                </destination>
        </rule>
        <separator>
                <wan/>
                <lan/>
                <floatingrules/>
        </separator>
        <bypassstaticroutes>yes</bypassstaticroutes>
</filter>
<shaper>
</shaper>
<ipsec/>
<aliases/>
<proxyarp/>
<cron>
        <item>
                <minute>1,31</minute>
                <hour>0-5</hour>
                <mday>*</mday>
                <month>*</month>
                <wday>*</wday>
                <who>root</who>
                <command>/usr/bin/nice -n20 adjkerntz -a</command>
        </item>
        <item>
                <minute>1</minute>
                <hour>3</hour>
                <mday>1</mday>
                <month>*</month>
                <wday>*</wday>
                <who>root</who>
                <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
        </item>
```

```
8411                <item>
8412                        <minute>*/60</minute>
8413                        <hour>*</hour>
8414                        <mday>*</mday>
8415                        <month>*</month>
8416                        <wday>*</wday>
8417                        <who>root</who>
8418                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
8419 sshlockout</command>
8420                </item>
8421                <item>
8422                        <minute>*/60</minute>
8423                        <hour>*</hour>
8424                        <mday>*</mday>
8425                        <month>*</month>
8426                        <wday>*</wday>
8427                        <who>root</who>
8428                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
8429 webConfiguratorlockout</command>
8430                </item>
8431                <item>
8432                        <minute>1</minute>
8433                        <hour>1</hour>
8434                        <mday>*</mday>
8435                        <month>*</month>
8436                        <wday>*</wday>
8437                        <who>root</who>
8438                        <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
8439                </item>
8440                <item>
8441                        <minute>*/60</minute>
8442                        <hour>*</hour>
8443                        <mday>*</mday>
8444                        <month>*</month>
8445                        <wday>*</wday>
```

```
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
virusprot</command>
                </item>
                <item>
                        <minute>30</minute>
                        <hour>12</hour>
                        <mday>*</mday>
                        <month>*</month>
                        <wday>*</wday>
                        <who>root</who>
                        <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
                </item>
        </cron>
        <wol/>
        <rrd>
                <enable/>
                <category>left=system-
processor&amp;right=&amp;resolution=300&amp;timePeriod=-
1d&amp;startDate=&amp;endDate=&amp;startTime=0&amp;endTime=0&amp;graphtype=line&amp;in
vert=true</category>
        </rrd>
        <load_balancer>
                <monitor_type>
                        <name>ICMP</name>
                        <type>icmp</type>
                        <descr><![CDATA[ICMP]]></descr>
                        <options/>
                </monitor_type>
                <monitor_type>
                        <name>TCP</name>
                        <type>tcp</type>
                        <descr><![CDATA[Generic TCP]]></descr>
                        <options/>
                </monitor_type>
                <monitor_type>
```

```
                        <name>HTTP</name>
                        <type>http</type>
                        <descr><![CDATA[Generic HTTP]]></descr>
                        <options>
                                <path>/</path>
                                <host/>
                                <code>200</code>
                        </options>
                </monitor_type>
                <monitor_type>
                        <name>HTTPS</name>
                        <type>https</type>
                        <descr><![CDATA[Generic HTTPS]]></descr>
                        <options>
                                <path>/</path>
                                <host/>
                                <code>200</code>
                        </options>
                </monitor_type>
                <monitor_type>
                        <name>SMTP</name>
                        <type>send</type>
                        <descr><![CDATA[Generic SMTP]]></descr>
                        <options>
                                <send/>
                                <expect>220 *</expect>
                        </options>
                </monitor_type>
        </load_balancer>
        <widgets>

        <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
/sequence>
        </widgets>
        <openvpn/>
```

```
        <dnshaper>
        </dnshaper>
        <unbound>
                <enable/>
                <dnssec/>
                <active_interface/>
                <outgoing_interface/>
                <custom_options/>
                <hideidentity/>
                <hideversion/>
                <dnssecstripped/>
        </unbound>
        <dhcpdv6>
                <lan>
                        <range>
                                <from>::1000</from>
                                <to>::2000</to>
                        </range>
                        <ramode>assist</ramode>
                        <rapriority>medium</rapriority>
                </lan>
        </dhcpdv6>
        <cert>
                <refid>5720a0502b277</refid>
                <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
                <type>server</type>

        <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXZ0F3SUJBZ0lCQURBTkJna3
Foa2lHOXcwQkFRc0ZBRENCdERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnTlZCQWdUQlZOMFlYUmxNUkV3RHdZ
RFZRUUhFd2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApaVzV6WlNCM1pXSkRiMjVtYVdkMWNtRjBiM0
lnVTJWc1ppMVRhV2R1WldRZ1EyVnlkR2xtYVdOaGRHVXhLREFtCkJna3Foa2lHOXcwQkNRRVdHV0ZrYldsdVFI
Qm1VMlZ1YzJVdWJHOWpZV3hrYjIxaGFXNHhIakFjQmdOVkJBTVQKRlhCbVUyVnVjMlV0TlRjeU1HRXdOVEF5WW
pJM056QWVGdzB4TmpBME1qY3hNVEU1TkRSYUZ3MHlNVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
d0pWVXpFT01Bd0dBMVVFQ0JNRlUzUmhkR1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNU1UZ3dOZ1lEVlFRS0
V5OXdabE5sYm5ObElIZGxZa052Ym1acFozVnlZWFJ2Y2lCVFpXeG0KTFZOcFoyNWxaQ0JEWlhKMGFXWnBZMkYw
WlRFb01DUdDU3FHU0liM0RRRUpBUllaWVdSdGFXNUFjR1pUWlc1egpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
dBMVVFQXhNVmNHWlRaVzV6WlMwMU56SXdZVEExTURKaU1qYzNNSUlCCklqQU5CZ2txaGtpRzl3MEJBUUVGQUFP
Q0FROEFNSUlCQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
hDODBHU0dhZnJENWdqcTRwZkNNMHlzbEFPaVlZK1hDYjdNa2o0dmtTMgpmbzl4emNyaDUrNVlaYlBHeXR1a2ls
ZWR4bjFWeFl6SllzYXZKdnlKb1lRMCtNTkx0dkFjYnRhTUFoZjh1ZkRFClhrclNVQ0N5YTFrbEYxNWJGZmcyUG
```

E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkUFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXd1SEZwd3J1LytYWExieEcrcD
dwYXI0aHR0UFRDcml1NmFqQVVTNmpvN05kOElQNWpzZ1kzR0h2ZjhzUUlECkFRQUJvNElCaGpDQ0FZSXdDUVlE
VlIwVEJBSXdBREFSQmdsZ2hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZSllJWkkKQVliNFFnRU5CQ1lXSkU5d1pXNV
RVMHdnUjJWdVpYSmhkR1ZrSUZObGNuWmxjaUJEWlhKMGFXWnBZMkYwWlRBZApCZ05WSFE0RUZnUVU3K1lLRmNp
OFFVSGhTZ0xEdjhFQ3NjQ0p3QUl3Z2VFR0ExVWRJd1NCMlRDQjFvQVU3K1lLCkZjaThRVUhoU2dMRHY4RUNzY0
NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsVlRNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
VUVCeE1JVEc5allXeHBkSGt4T0RBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaQpRMjl1Wm1sbmRYSmhkRzl5SU
ZObGJHWXRVMmxuYm1Wa0lFTmxjblJwWm1sallYUmxNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
bE5sYm5ObExteHZZMkZzWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
56ZUNBUUF3SFFZRFZSMGxCQll3RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd0lG
b0RBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZFpQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmtNaTB5M0
9PWGtzWEs1cEM2dTd6Ukl3WjEvRjYyRUp3ODlUOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWJhRU42NEkxOHFud3Zm
S2JrREZvRThMR1hSdzBkMnAyTGVmYTd4YTIvSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG
c4bGdrcVc3dStlb01DNDJIbVJkOURCTmlzdFJ4RVlNMkFLQkFsZG1LYStvRUY1VUwwCm43aXpvNlZ4dHJWMTJv
TTdySllRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VVnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOVpPSmR2QmZLVU
1sUWlELyswSVpTalFXRDczWkdsaEhTK2tOeWc1aDJhUjUwYjh3Wm9zQnNjSUZDa0pFbgp0UT09Ci0tLS0tRU5E
IENFUlRJRklDQVRFLS0tLS0K</crt>

<prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z0lCQURBTkJna3Foa2lHOXcwQkFRRU
ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M0lhYlkKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4
eGxiY3UyRUx6UVpJWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMWitqM0hOeXVIbjdsaGxzOG
JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcwdTI4Qnh1CjFvd0NGL3k1OE1SZVN0SlFJTEpyV1NVWFhs
c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcwdkEKQVdEQkQzNDg5OHRUalhROVNpb1NaclREbn
dKTmo3cHAwQnM4ZHhlRDBjL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
dHZFYjZudWxxdmlHMjA5TUt1SzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUpRRF
pxU3duMnNTUTh0SVNBTUVrUW0zcXhrb3BzdzB4cWNScmFlOEd4VmQKejBpOU1KbkZVQWFleTQvL3Jldndh ZW1P
R3RYSmZ2ai9jSnY3cmJIWGIzYkJtVW9hcDhxY0RjdnVSMmlHRUZYWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcD
lzNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1ZnlP
UzAvbXlmNU5YLzVoRklPNmFDc0xlUjZ4N1RZa2FDQU9FYlViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
hMZ0NRYlB2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUE0NzNMUWoxcExLSmRZN2JxCmtMU3NVT0ZhTUZlZG1xU2ttbzh3Qj
lpMXhzbElLQUd0M3U4dTdMZlZtU2lybnMwVVBTMHRVUDRyQXMzVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
OGttbFJnUFRmVHVPaGNwMGVkamQwK1E5Y2VlY25kaFp3UEl6TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHNhbm
NBRDhVYThDZ1lFQXpzYjYzbzRBSHlYNjZkcEJ6TGlzYzZxS2d2ZG4xazhVCm02N3RuK2M3NkVhSEtZTlk0Rjdh
S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUpOK0I3Sm
Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZm1DWlpRSUQ1OENnWUJjamFO
dk5obnFJOG9rWGhBUjR2c3NtNGpWb0tYU1ZScjRIVHo5MDFwOGdReXNCWkt0CnlUS2V6VThuUVZvTjNYWmVMbC
8rVEcwYVpKOTZHKy9nNTRWZmZqWTRlelVScHhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
QWY5Mi9CbHZJR25FS1pMdnhLWTdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
RG1hZGsvKy9Ud2UvVk1Kbmx2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUjlhbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBRS0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1Rlczdu
WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLClUzSThhYnpnUUtwOEwrZj
VadTAxY1pZVk5TU0FIUFRHYm5jb1IzbGVPYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>

</cert>

<revision>

<time>1493655499</time>

<description><![CDATA[admin@10.97.67.135: /firewall_rules_edit.php made unknown change]]></description>

<username>admin@10.97.67.135</username>

</revision>

<gateways>

```
8611                <gateway_item>
8612                      <interface>wan</interface>
8613                      <gateway>192.168.13.1</gateway>
8614                      <name>GW_WAN_2</name>
8615                      <weight>1</weight>
8616                      <ipprotocol>inet</ipprotocol>
8617                      <interval/>
8618                      <descr><![CDATA[Interface wan Gateway]]></descr>
8619                </gateway_item>
8620                <gateway_item>
8621                      <interface>wan</interface>
8622                      <gateway>192.168.13.19</gateway>
8623                      <name>GW_VLAN19</name>
8624                      <weight>1</weight>
8625                      <ipprotocol>inet</ipprotocol>
8626                      <descr><![CDATA[Gateway to VLAN 19]]></descr>
8627                </gateway_item>
8628          </gateways>
8629          <ppps/>
8630          <dyndnses/>
8631          <virtualip>
8632                <vip>
8633                      <mode>ipalias</mode>
8634                      <interface>wan</interface>
8635                      <uniqid>57bf05ffdcc3c</uniqid>
8636                      <descr><![CDATA[VIP mapping to ConsoleWorks]]></descr>
8637                      <type>single</type>
8638                      <subnet_bits>32</subnet_bits>
8639                      <subnet>192.168.13.171</subnet>
8640                </vip>
8641          </virtualip>
8642    </pfSense>
```

Appendix A List of Acronyms

AD Active Directory

ARM Access Rights Management

CA Certificate Authority

CSF Cybersecurity Framework

FBA Forms Based Authentication

GPO Government Printing Office, Group Policy Object (depending on context)

GUI Graphical User Interface

HTCC HyTrust CloudControl

IdAM Identity and Access Management

IT Information Technology

LDAP Lightweight Directory Access Protocol

LDAPS Lightweight Directory Access Protocol (Secure)

NCCoE National Cybersecurity Center of Excellence

NIST National Institute of Standards and Technology

PEP Policy Enforcement Point

RMF Risk Management Framework

SA Situational Awareness

SCM Security Compliance Manager

SIEM Security Information and Event Management

RDP Remote Desktop Protocol

VD Virtual Directory

VDS Virtual Directory System

VM Virtual Machine

VNC Virtual Network Computing

VPN Virtual Private Network