

## 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](mailto: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](mailto:nccoe@nist.gov)

## 1 **NATIONAL CYBERSECURITY CENTER OF EXCELLENCE**

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

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

## 16 **NIST CYBERSECURITY PRACTICE GUIDES**

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

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

## 26 **ABSTRACT**

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

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

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

## 56 **KEYWORDS**

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

## 58 **ACKNOWLEDGMENTS**

59 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

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

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

## 65 **Contents**

66	<b>1 Introduction .....</b>	<b>1</b>
67	1.1 Practice Guide Structure .....	1
68	1.2 Build Overview .....	2
69	1.3 Typographical Conventions .....	2
70	1.4 Logical Architecture Summary .....	3
71	1.5 Network Diagrams .....	4
72	1.6 NCCoE Lab.....	4
73	<b>2 Product Installation Guides.....</b>	<b>7</b>
74	2.1 AlertEnterprise .....	7
75	2.1.1 How It's Used .....	7
76	2.1.2 Virtual Machine Configuration.....	7
77	2.1.3 Prerequisites .....	8
78	2.1.4 Java .....	8
79	2.1.5 Apache ActiveMQ.....	8
80	2.1.6 Oracle DB .....	9
81	2.1.7 7-Zip .....	9
82	2.1.8 Installation .....	9
83	2.1.9 Install and Configure Tomcat .....	10
84	2.1.10 Configure the Database Server .....	10
85	2.1.11 Deploying the Application.....	11
86	2.1.12 Start the Server .....	12
87	2.1.13 Provisioning Configuration.....	12
88	2.1.14 Creating System Connectors .....	12
89	2.1.15 User Data Source .....	15
90	2.1.16 Process Designer .....	15
91	2.1.17 Policies .....	16
92	2.1.18 Rules .....	17

93	2.1.19 Policy Designer .....	17
94	2.1.20 Triggers Field Map .....	19
95	2.1.21 Form Customization.....	20
96	2.1.22 User Field Mapping.....	20
97	2.1.23 Provisioning Mapping .....	21
98	2.1.24 External Provisioning Attributes.....	23
99	2.1.25 Role Repository .....	23
100	2.1.26 Enabling SSL.....	25
101	2.2 HyTrust Cloud Control .....	25
102	2.2.1 How Its Used .....	25
103	2.2.2 Virtual Machine Configuration.....	26
104	2.2.3 Installing Vcenter Server .....	26
105	2.2.4 Configuring Vcenter Server .....	27
106	2.2.5 Deploying HTCC .....	27
107	2.2.6 Configuring HTCC.....	27
108	2.2.7 Integrating With Active Directory.....	32
109	2.2.8 Creating and Deploying Access Policies.....	34
110	2.2.9 Configure Logging.....	36
111	2.3 Microsoft Active Directory .....	37
112	2.3.1 How It's Used .....	37
113	2.3.2 Virtual Machine Configuration.....	37
114	2.3.3 Installing AD .....	38
115	2.3.4 DNS Configuration .....	38
116	2.3.5 Installing Splunk Universal Forwarder .....	38
117	2.3.6 Install Security Compliance Manager .....	39
118	2.3.7 Group Policy Object (GPO) Configuration.....	39
119	2.3.8 Script: AdDOonlineStatus.ps1 .....	47
120	2.3.9 LDAPS Configuration.....	48
121	2.4 NextLabs Entitlement Manager .....	50

122	2.4.1	How It's Used .....	50
123	2.4.2	Virtual Machine Configuration.....	50
124	2.4.3	Prerequisites .....	51
125	2.4.4	Installing NextLabs.....	51
126	2.5	OpenLDAP.....	68
127	2.5.1	How It's Used .....	68
128	2.5.2	Virtual Machine Configuration.....	68
129	2.5.3	Firewall Configuration.....	69
130	2.5.4	Installation .....	69
131	2.5.5	Audit Configuration .....	70
132	2.5.6	STARTTLS and LDAPS Configuration .....	71
133	2.5.7	Formatting Audit Logs.....	73
134	2.5.8	Script: /etc/ldap/logs/auditlogscript .....	73
135	2.5.9	Script: /etc/ldap/logs/add-timestamp.py.....	73
136	2.5.10	Script: /etc/cron.daily/openldap-status .....	74
137	2.6	Radiant Logic.....	74
138	2.6.1	How Its Used .....	74
139	2.6.2	Virtual Machine Configuration.....	74
140	2.6.3	Installing the Virtual Directory .....	75
141	2.6.4	Configuring VD .....	75
142	2.6.5	Configure Logging.....	80
143	2.6.6	Configure Views for SharePoint .....	84
144	2.6.7	Scripts .....	90
145	2.6.8	Script: RadiantOnlineStatus.ps1 .....	92
146	2.6.9	Script: VanguardOnlineStatus.ps1.....	93
147	2.6.10	LDAPS Configuration.....	94
148	2.7	SharePoint .....	94
149	2.7.1	How It's Used .....	94
150	2.7.2	Virtual Machine Configuration.....	94

151	2.7.3	Prerequisites .....	95
152	2.7.4	Installing SharePoint 2013 .....	95
153	2.7.5	Configuring SharePoint.....	95
154	2.7.6	Web Configs .....	97
155	2.8	Splunk .....	102
156	2.8.1	How It's Used .....	102
157	2.8.2	Installation .....	102
158	2.8.3	Queries.....	103
159	2.8.4	Query: Detect User Provisioning Accounts Events.....	103
160	2.8.5	Query: Authorized and Unauthorized Provisioning Trend Line Chart .....	104
161	2.8.6	Query: Combined Provisioning Trend Line Chart .....	105
162	2.8.7	Query: Detect modifications to High Value or Privileged Accounts .....	106
163	2.8.8	Query: Virtual Directory Server Offline Detection .....	107
164	2.8.9	Query: Critical Servers Offline.....	107
165	2.8.10	SSL Forwarding .....	107
166	2.9	TDI ConsoleWorks .....	108
167	2.9.1	How It's Used.....	108
168	2.9.2	Virtual Machine Configuration.....	108
169	2.9.3	Firewall Configuration.....	109
170	2.9.4	Installation .....	109
171	2.9.5	Console Connection Configuration.....	109
172	2.9.6	Graphical Gateway Configuration .....	109
173	2.9.7	Graphical Connection Configuration .....	110
174	2.9.8	Profile Creation.....	110
175	2.9.9	Access Controls.....	111
176	2.9.10	User Auditing.....	117
177	2.9.11	Cron Configuration: /etc/crontab.....	117
178	2.9.12	Scripts: connectionreporting.....	117
179	2.9.13	Scripts: bashconnectionreporting .....	118

180	2.10 Network Firewall Configuration.....	118
181	2.10.1 Firewall Configuration for Backbone Subnet .....	119
182	2.10.2 Firewall Configuration for Common Services Subnet.....	177
183	2.10.3 Firewall Configuration for ID-ARM Subnet .....	209
184	2.10.4 Firewall Configuration for Private Cloud Subnet.....	245
185	2.10.5 Firewall Configuration for the Management and Monitoring Subnet.....	265
186	<b>Appendix A List of Acronyms .....</b>	<b>297</b>
187		

## 188 **List of Tables**

189	<b>Table 1-1 NCCoE Lab Network and System IP Addresses .....</b>	<b>6</b>
-----	--	----------

## 190 **List of Figures**

191	<b>Figure 1-1 Logical Access Rights Management Lab Build Architecture .....</b>	<b>4</b>
192	<b>Figure 1-2 Logical Security Log Collection and Monitoring Lab Build Architecture.....</b>	<b>4</b>
193	<b>Figure 1-3 NCCoE Lab Networking Diagram .....</b>	<b>5</b>
194	<b>Figure 1-4 NCCoE Lab Networking Diagram .....</b>	<b>6</b>

## 195 1 Introduction

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

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

### 203 1.1 Practice Guide Structure

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

207 The guide contains three volumes:

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

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

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

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

218 **Technology or security program managers** who are concerned with how to identify, understand, assess,  
219 and mitigate risk will be interested in the *Approach, Architecture, and Security Characteristics* (NIST SP  
220 1800-9b) part of the guide, which describes what we did and why. The following sections will be of  
221 interest:

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

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

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

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

240 A *NIST Cybersecurity Practice Guide* does not describe "the" solution, but a possible solution. This is a  
 241 draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and  
 242 success stories will improve subsequent versions of this guide. Please contribute your thoughts to  
 243 [financial\\_nccoe@nist.gov](mailto:financial_nccoe@nist.gov).

## 244 1.2 Build Overview

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

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

## 259 1.3 Typographical Conventions

260 The following table presents typographic conventions used in this volume.

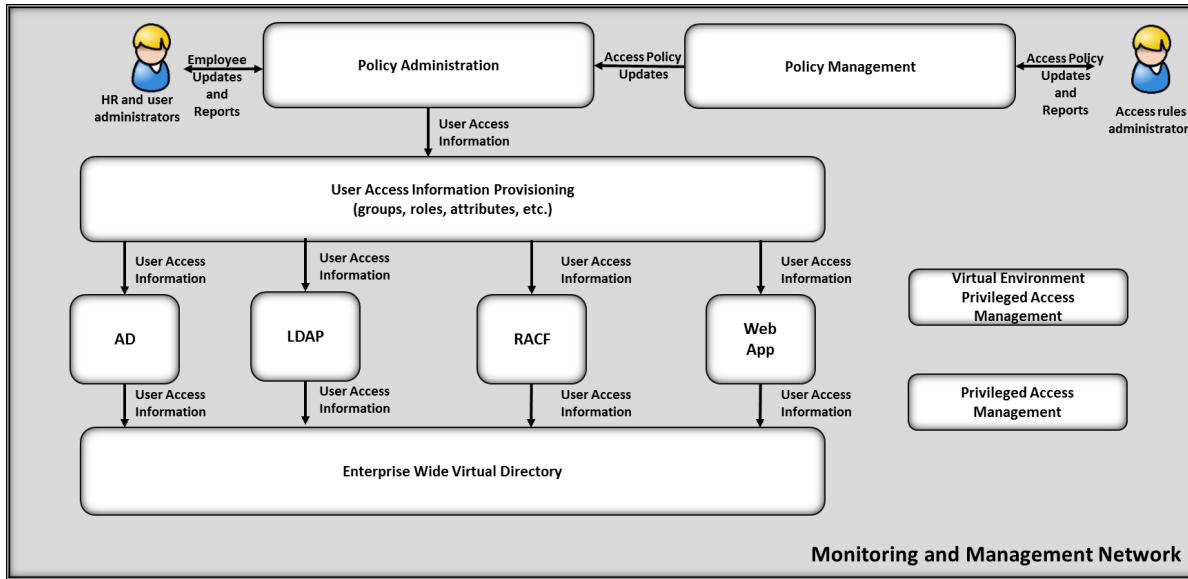
Typeface/ Symbol	Meaning	Example
<i>Italics</i>	filenames and pathnames	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .

Typeface/ Symbol	Meaning	Example
	references to documents that are not hyperlinks, new terms, and placeholders	
<b>Bold</b>	names of menus, options, command buttons and fields	Choose <b>File &gt; Edit.</b>
Monospace	command-line input, on-screen computer output, sample code examples, status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<b>service sshd start</b>
<u>blue text</u>	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 <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a>

261    **1.4 Logical Architecture Summary**

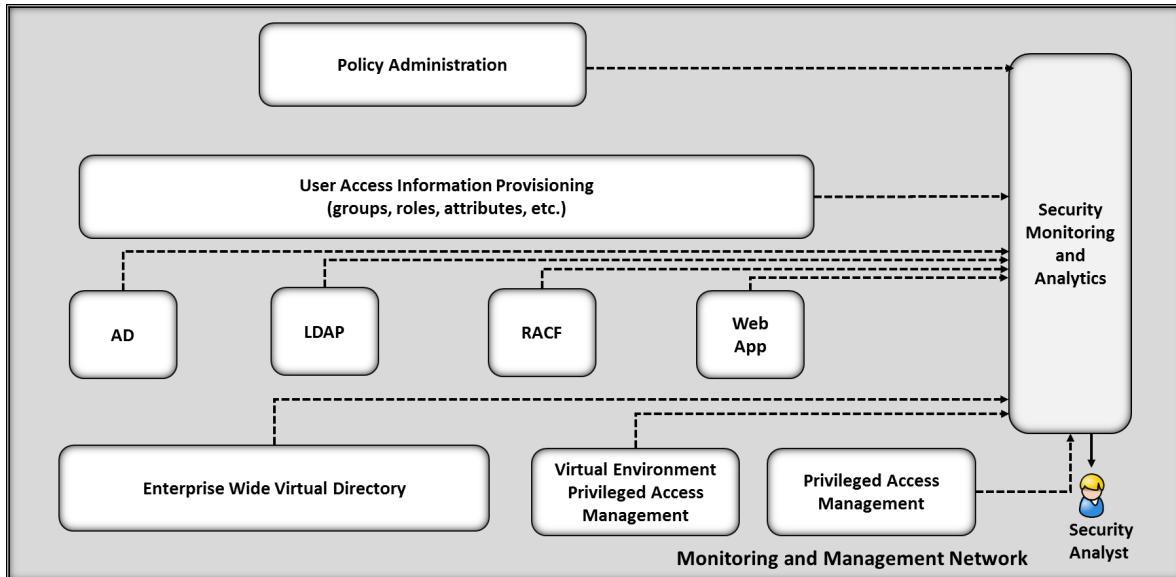
262    NIST Special Publication 1800-9b (SP1800-9b) describes an example implementation consisting of user  
 263    access management (including provisioning) and security monitoring / data collection. SP1800-9b  
 264    includes a much more detailed description of the architecture for building an instance of the example  
 265    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.

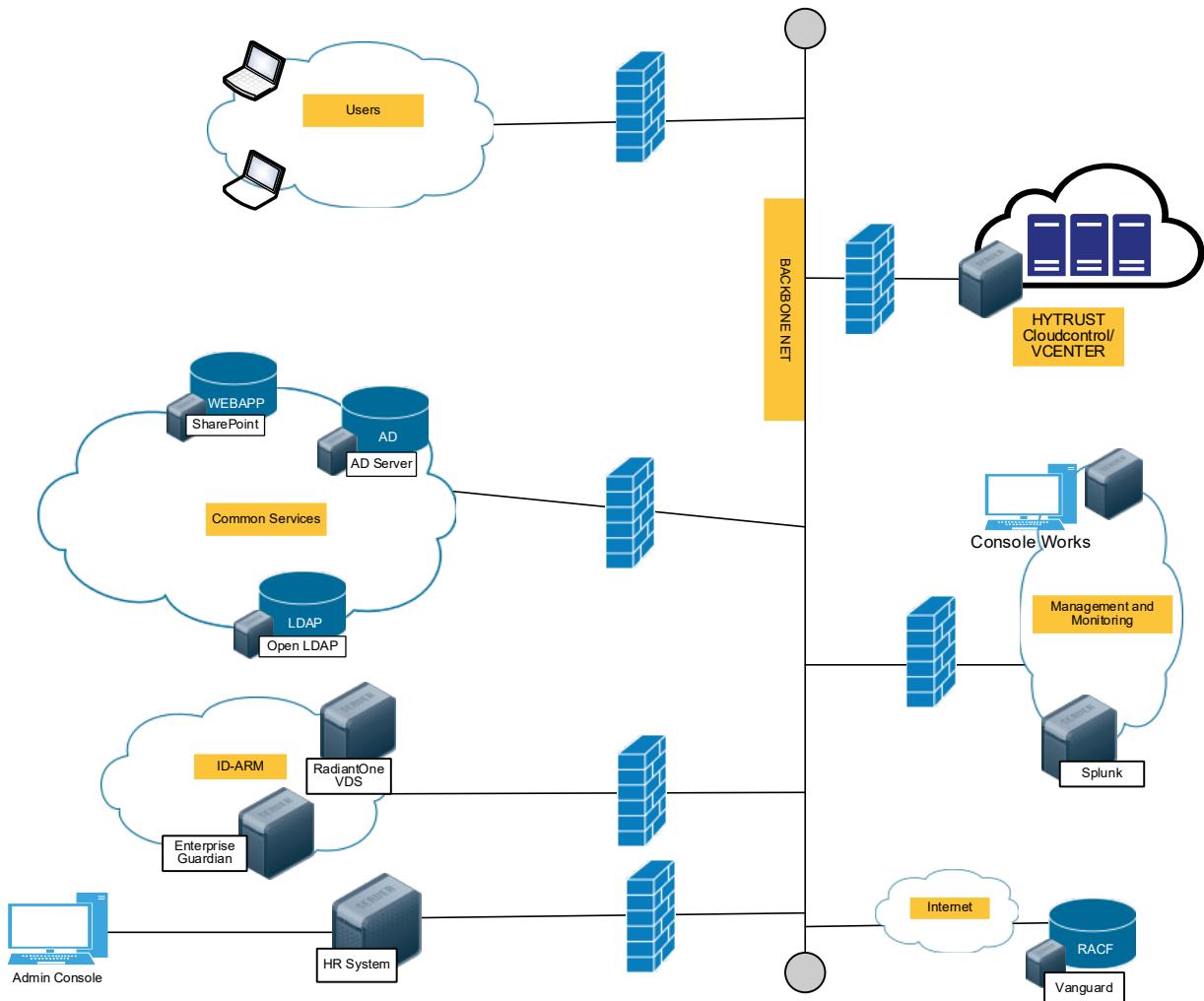
## 273 1.5 Network Diagrams

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.

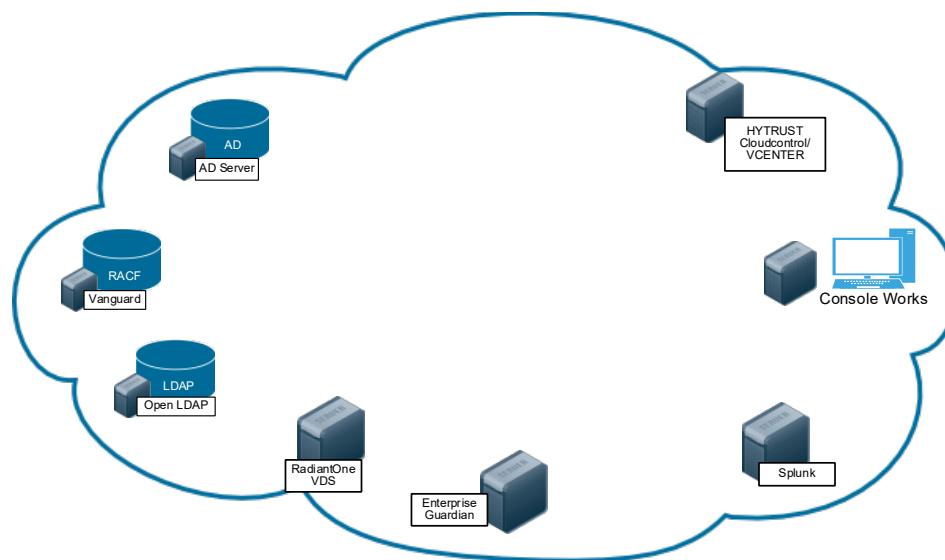
## 277 1.6 NCCoE Lab

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. Provisioning 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

322    **2.1.3 Prerequisites**

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

327    Prerequisite software used in this build:

- 328        ▪ JRE 1.6 Update 22  
329        ▪ Apache Tomcat 6.0.26  
330        ▪ Oracle SQL Database 12c  
331        ▪ Google Chrome 55.0.2883.87  
332        ▪ 7-zip 16.04

333    **2.1.4 Java**

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

339            **Set JAVA\_HOME=<PATH OF JDK/JRE>**

340            Where <> is the path where Java is installed, for example,  
341            C:\Program Files\Java\JRE6

- 342        4. Setting Path:  
343            PATH= C:\Program Files\Java\JDK1.6.0-21\bin;%PATH%
- 344        5. Checking JAVA\_HOME and PATH:  
345            Echo %JAVA\_HOME%  
346            Echo %PATH%

347    **2.1.5 Apache Activemq**

- 348        1. Install the Activemq server according to documentation found on the Apache [website](#).
- 349        2. Run ActiveMQ as a Windows service.
- 350        3. Ensure the server is installed correctly and running by connecting to the admin console on port  
351            8161. For example: URL: <IP address of the server where Active MQ is 2130

352

installed&gt;:8161/admin

The screenshot shows the Apache ActiveMQ Admin Console interface. At the top, there are several tabs: 'localhost: ActiveMQ Con...', 'Apache Tomcat', 'NIST', 'https://support.alertente...', and 'Local Naming Parameters'. The main content area displays the 'Broker' status for 'localhost'. It includes a table with the following data:

Name	localhost
Version	5.6.0
ID	ID:WIN-CHSUIS3NKVR-13184-1485437798384-0:1
Store percent used	0
Memory percent used	0
Temp percent used	0

On the right side, there is a sidebar titled 'Support' with links to 'Queue Views', 'Topic Views', 'Subscribers Views', and 'Useful Links'.

353

## 2.1.6 Oracle DB

- 355 1. Install the Oracle SQL database according to documentation found on the Oracle [website](#).
- 356 2. Ensure the pdborcl pluggable database service name is added correctly in the tnsnames.ora file per the Oracle documentation.

```
# tnsnames.ora Network Configuration File: C:\app\OracleHomeUser1\product\12.1.0\dbhome_1\network\admin\tnsnames.ora
# Generated by Oracle configuration tools.

LISTENER_ORCL1 =
  (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))

ORACLE_CONNECTION_DATA =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
    (CONNECT_DATA =
      (SID = CLRExtProc)
      (PRESENTATION = RO)
    )
  )

ORCL1 =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = orcl1)
    )
  )

PDBORCL =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = localhost)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = pdborcl)
    )
  )

```

358

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

## 2.1.7 7-Zip

- 362 1. Download and install 7-Zip from [www.7-zip.org](http://www.7-zip.org).

## 2.1.8 Installation

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

- 366 1. Install and Configure the Apache Tomcat Server.

- 367           2. Configure the database server.
- 368           3. Deploy the application.

## 369 2.1.9 Install and Configure Tomcat

## 382 2.1.10 Configure the Database Server

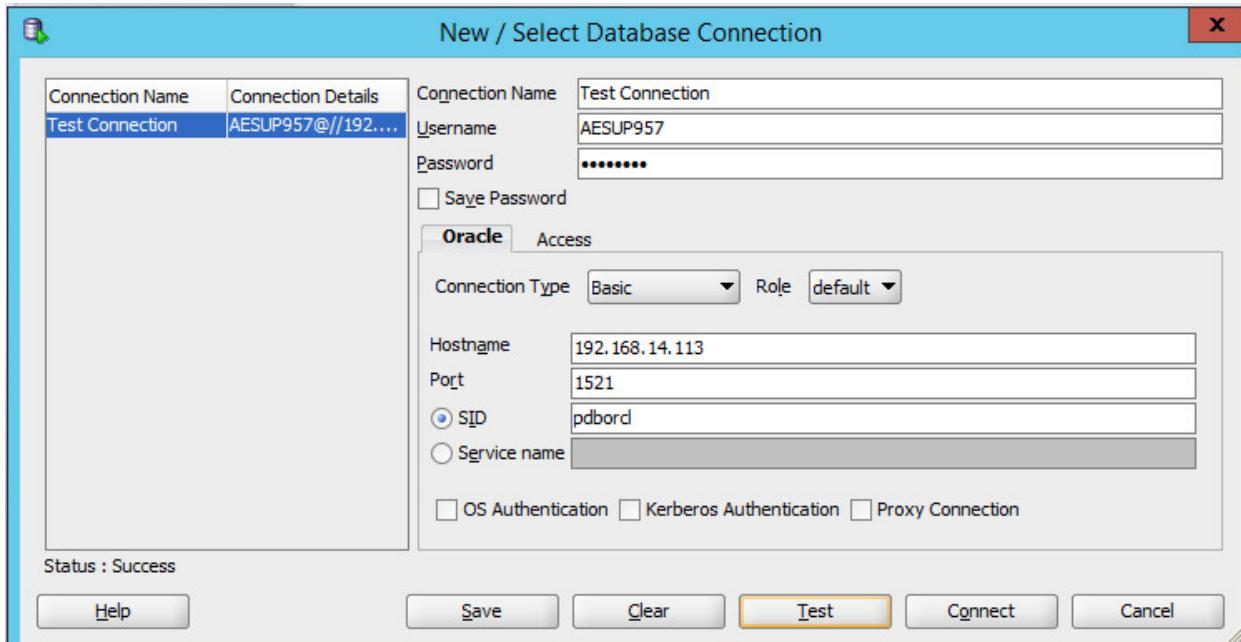
383 The NCCoE build supports Oracle SQL Database 12c. See the administrator's guide for the full installation  
384 and configuration guide. Open a command prompt with administrator privileges and connect: `sqlplus`  
385 `sys/<password>@pborcl as sysdba`

386     1. Create a new schema/SID per your naming convention: `create user <user/schema name>`  
387         `identified by <password>`, you may have to unlock the schema: `alter user`  
388         `<user/schema name> identified by <password> unlock`

389     2. Use `grant <attribute> to <user/schema name>`; to grant the new user all of the  
390         following attributes:

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

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



395

### 2.1.11 Deploying the Application

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

398  
 399 *Note:* For steps required to use the SAP system connector or MySQL database, see the vendor  
 400 documentation.

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

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

## For ORACLE:

```
422 <Resource description="DB Connection"  
423 name="jdbc/alntdb" auth="Container"  
424 type="com.mchange.v2.c3p0.ComboPooledDataSource"  
425 factory="org.apache.naming.factory.BeanFactory"  
426 user=<"Schema User">  
427 password=<"Schema User Password">  
428 jdbcUrl="jdbc:oracle:thin:@<db host name>:<db port>:<schema name>/SID"  
429 driverClass="oracle.jdbc.driver.OracleDriver" maxPoolSize="100"  
430 minPoolSize="5"  
431 acquireIncrement="5"  
432 numHelperThreads="20"  
433 maxIdleTime="600"  
434 maxIdleTimeExcessConnections="300"  
435 debugUnreturnedConnectionStackTraces="true"  
436 ignoreInitialTimeout="true" />
```

<sup>8</sup>. 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`.

442                  Note: 8080 is the default port on local host. If you want to change it, change it in the  
443                  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

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

## 2.1.14 Creating System Connectors

- 453        1. Navigate to **Setup > Manual Configuration > Systems > System**.  
454        2. Click **New** to create a new system.  
455        3. Enter the following Definition:  
456              a. System Type – Active Directory  
457              b. Connector Name – AD  
458              c. Connector Description – AD  
459              d. Connector Long Description – AD  
460              e. Connector Type – LDAP (default)  
461        4. Click **Next**.

- 462 5. Enter the following Parameters:

463 a. HostName – 192.168.19.10

464 b. Port Number – 636 (use 389 if SSL is not configured yet)

465 c. Service user Dn – CN=AlertServiceAccount,CN=Users,DC=Acmefinancial,DC=com

466 d. Password – Fsarm@nccoe1

467 e. Use SSL – true (use false if SSL is not configured yet)

468 f. User Base DN – OU=Operations,DC=Acmefinancial,DC=com

469 g. Group Base DN – DC=Acmefinancial,DC=com

470 h. Object Class – user

471 i. Is Primary – Yes

472 j. LastModified Column role – whenChanged

473 k. Last Modified User Column – whenChanged

474 6. Click **Next**.

475 7. Enter the following parameters:

476 a. Application – AlertAccess

477 b. Check the following boxes – Provisioning, Role Management, Offline System, Allow Modify Role

478 c. Category – production

479 d. Time Zone – Eastern Standard Time

480 8. Click **Next**.

481 9. Click **Save**.

482 10. Repeat Steps 1–9 to add the OpenLDAP and RACF connectors with the following parameters:

483 OpenLDAP:

484 a. System Type – OpenLDAP Server

485 b. Connector Name – OPENLDAP

486 c. Connector Description – OpenLDAP

487 d. Connector Type – OpenLDAP

488 e. HostName – 192.168.19.11

489 f. Port Number – 636 (use 389 if SSL is not configured yet)

490 g. Service user Dn – CN=Admin,DC=Acmefinancial,DC=com

491 h. Password – Fsarm@nccoe1

492 i. Use SSL – true (use false if SSL is not configured yet)

493 j. User Base DN – OU=Operations,DC=Acmefinancial,DC=com

494 k. Group Base DN – OU=Operations,DC=Acmefinancial,DC=com

495 l. Object Class – inetOrgPerson

496 m. Group Object Class Name – groupOfUniqueNames

497 n. Primay Connection – Yes

498 o. LastModified Column role – whenChanged

499 p. Last Modified User Column – whenChanged

500 q. Member Attribute Name for Group – uniqueMember

501 r. LDAP DnName – cn

502 s. LDAP Account Control Column Name – cn

503 t. User Password attributed – default

504 u. Encode Password Required? – default

505 v. LDAP Group Search Attributed – cn

- 507                   w. **userIdColumnName (Optional Parameter)** - cn  
508                   x. **Application** – AlertAccess  
509                   y. **Check the following boxes** – Provisioning, Role Management, Offline System,  
510                   Allow Modify Role  
511                   z. **Category** – production  
512                   aa. **Time Zone** – Eastern Standard Time  
513                   **RACF:**  
514                   a. **System Type** – OpenLDAP Server  
515                   b. **Connector Name** – RACF\_OPENLDAP  
516                   c. **Connector Description** – RACF\_OpenLDAP  
517                   d. **Connector Type** – OpenLDAP  
518                   e. **HostName** – 172.17.212.10  
519                   f. **Port Number** – 636 (use 389 if SSL is not configured yet)  
520                   g. **Service user Dn** – racfid=TSNI00,profiletype=user,sysplex=sysplex1  
521                   h. **Password** – Fsarm@nccoe1  
522                   i. **Use SSL** – true (use false if SSL is not configured yet)  
523                   j. **User Base DN** – profiletype=user,sysplex=sysplex1  
524                   k. **Group Base DN** – profiletype=user,sysplex=sysplex1  
525                   l. **Object Class** – racfUser  
526                   m. **Primay Connection** – Yes  
527                   n. **LDAP DnName** – racfId  
528                   o. **LDAP UserID Column Name** – racfId  
529                   p. **User Password attributed** – default  
530                   q. **Encode Password Required?** – default  
531                   r. **Ignore user check** – Yes  
532                   s. **isObjectClassExist** – No  
533                   t. **userIdColumnName (Optional Parameter)** – racfid  
534                   u. **isCnAttrExists (Optional Parameter)** – No  
535                   v. **Application** – AlertAccess  
536                   w. **Check the following boxes** – Provisioning, Role Management, Offline System,  
537                   Allow Modify Role  
538                   x. **Time Zone** – Eastern Standard Time  
539                   **File Connector**  
540                   a. **System Type** – File Connector  
541                   b. **Connector Name** – FILE CONNECTOR  
542                   c. **Connector Type** – FileConnector  
543                   d. **User Folder Path** – C:\Program Files\User  
544                   e. **Role Folder Path** – C:\Program Files\Role  
545                   f. **User role Folder Path** – C:\Program Files\UserRole  
546                   g. **Column Header for User ID** – UserId  
547                   h. **Skip Provisioning** – Yes  
548                   i. **Application** – AlertAccess  
549                   j. **Check the following boxes** – Provisioning, Role Management  
550                   k. **Category** – Production  
551                   l. **Time Zone** – Eastern Standard Time

552            Identity Store  
 553            a. System Type – Database (JDBC J2EE)  
 554            b. Connector Name – IDENTITYSTORE  
 555            c. Connector Type – Database (JDBC J2EE)  
 556            d. User Name – admin  
 557            e. Password – System@123  
 558            f. JNDI Name – java:comp/env/jdbc/alntdb  
 559            a. Application – Alert Access  
 560            b. Check the following boxes – Provisioning, Role Management, Offline System,  
 561            Identity Provider  
 562            g. Category – Production  
 563            h. Time Zone – Eastern Standard Time

### 2.1.15 User Data Source

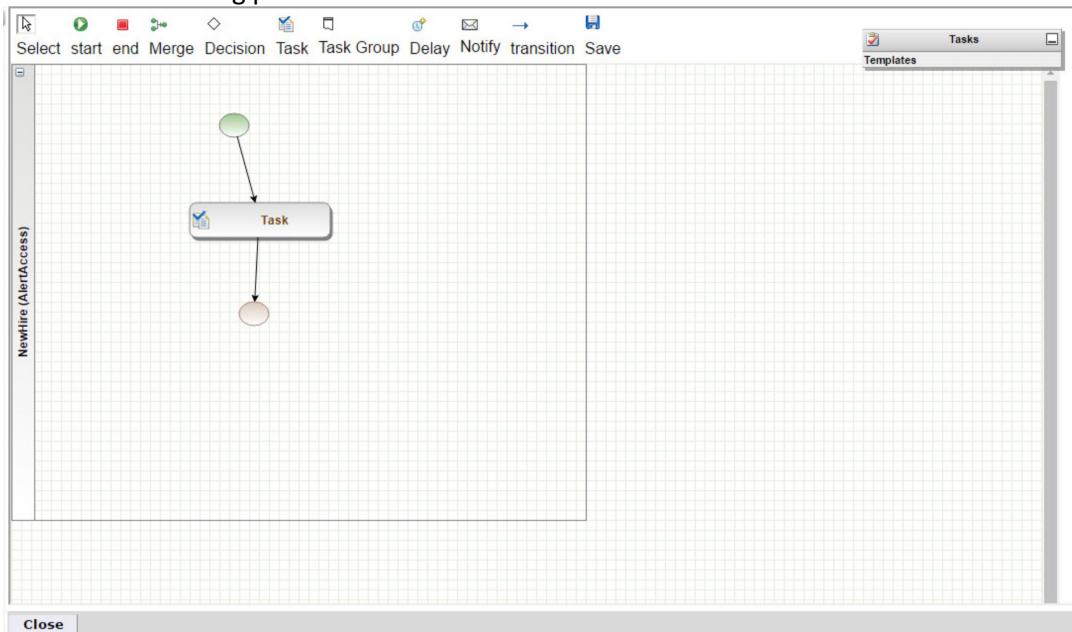
- 564        1. Navigate to **Setup>Manual Configuration>User Data>User Data Source.**
- 565        2. Click **New**. Create the following User Data Source:

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

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

- 571 4. Create the following process:



572

### 2.1.17 Policies

- 574 1. Navigate to **Setup>Manual Configuration>Policy Engine>Policies**.
- 575 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

576

577 **2.1.18 Rules**

- 578 1. Navigate to **Setup>Manual Configuration>Policy Engine>Rules**.  
 579 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 Assignment	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

580 **2.1.18.1 Suggest/Default Access**

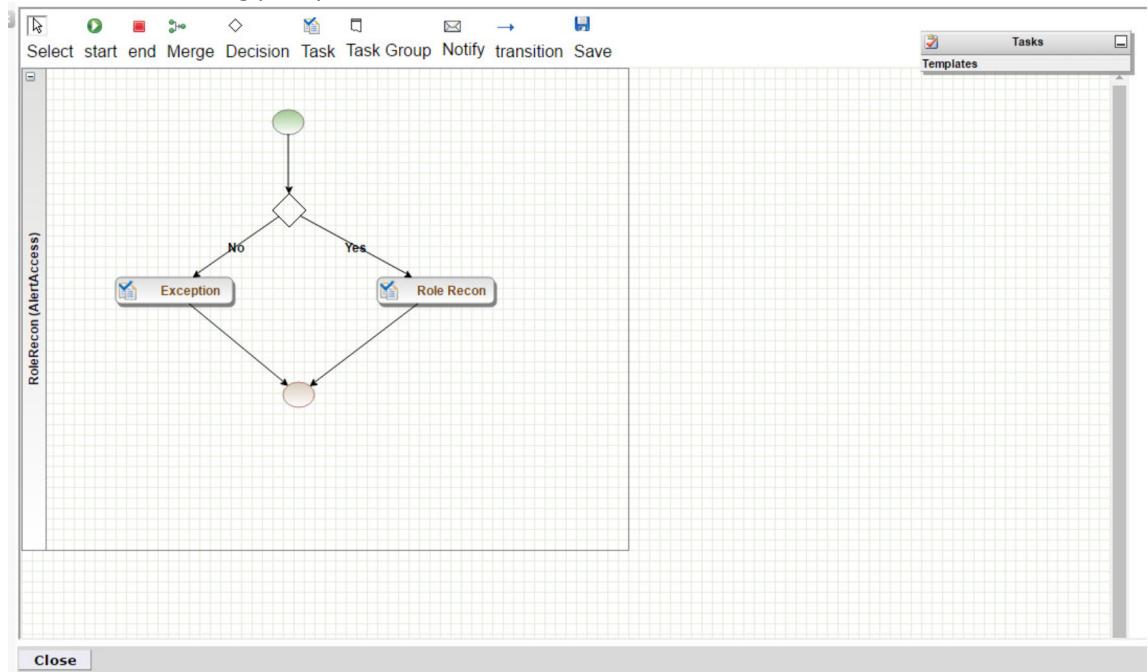
- 581 1. Navigate to **Setup>Manual Configuration>Policy Engine>Suggest/Default Access**.  
 582 2. Click **New**. Create the following criteria:

Name	Type	Condition	Search By	Resources	Attributes
NewHire	Default	NewHireSuggestDefault	Systems	OpenLDAP, AD, RACF_OPENLDAP	
DefaultRoleAssignment	Default	NewHireSuggestDefault	Role Attributes		Alias
123	Default	NewHireSuggestDefault	Role Attributes		RoleDescription

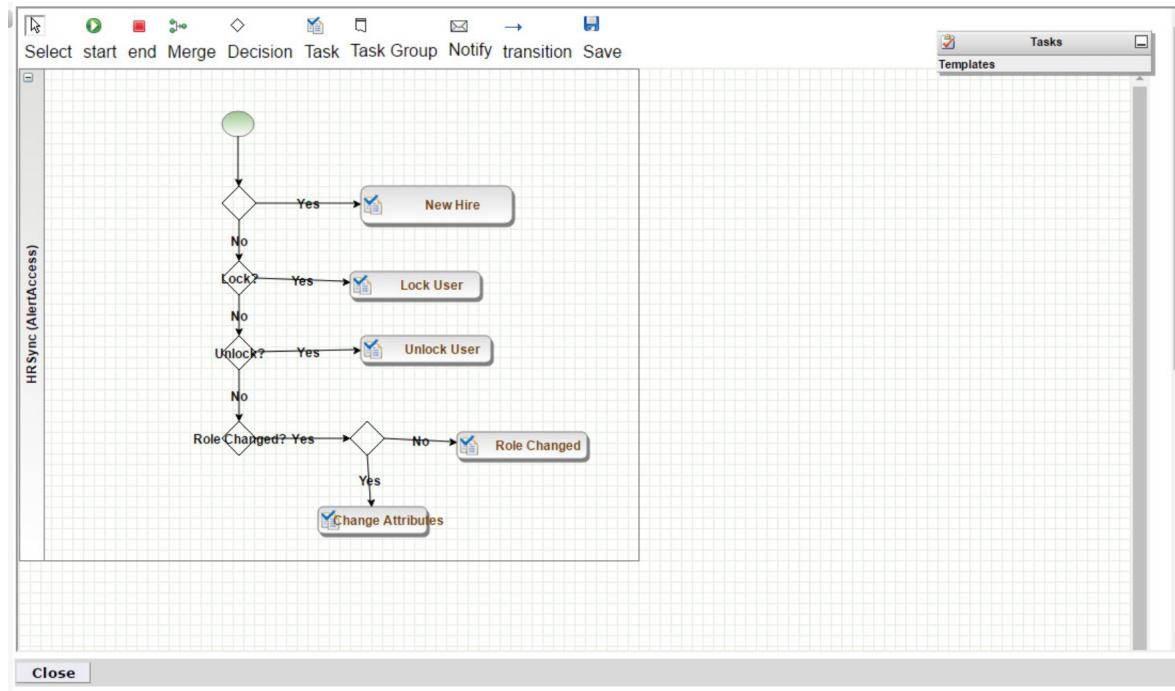
583 **2.1.19 Policy Designer**

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

- 587 4. Create the following policy:



- 588 589 5. Repeat Steps 1-4 for with HRSync as the **Name** and the following policy:



590

#### 591 2.1.19.1 Rule Action Handlers

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

Action Handler Name	Workflow	Task Type	Value	Priority	Update Identity Info	Evaluate Enterprises Role
Termination	AlertAccess	Recon Create Request	Termination	0	Yes	No
Recon Exception	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		
ChangeAccess	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

594 [\*2.1.19.2 Job Triggers\*](#)

595 1. Navigate to **Setup>Manual Configuration>Job Scheduler>Triggers**.

596 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

597 [\*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:

Group Name	Type
HR Sync	Reconciliation

### 2.1.21 Form Customization

- 601     1. Navigate to **Setup>Manual Configuration>Form Customization>Attributes**.  
 602     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
Racfworkatusername	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.

### 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

### 610 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:

### 614 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

### 615 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

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

616

**AD**

Directory Attribute Name	Mandatory	AlertEnterprise Attribute Name	Default Value	Editable	Visible	Validation Flag	isUser-Id attribute
<b>sAMAccountName</b>	No	ADUserId		Yes	Yes	No	Yes
<b>Sn</b>	No	LastName		Yes	Yes	No	No
<b>givenName</b>	No	FirstName		Yes	Yes	No	No
<b>accountExpires</b>	No	ValidTo		Yes	Yes	No	No
<b>UserBaseDn</b>	No	User Base Dn		Yes	Yes	No	No
<b>unicodePwd</b>	No	Password	System@123	Yes	Yes	No	No
<b>displayName</b>	No	DispalyName	\$(Lastname), \$(FirstName)	Yes	Yes	No	No
<b>Mail</b>	No	Email		Yes	Yes	No	No
<b>employeeNumber</b>	No	EmployeeNo		No	No	No	No
<b>Mobile</b>	No	Mobile		No	No	No	No
<b>Department</b>	No	Department		No	No	No	No
<b>userPrincipalName</b>	No	NISTEmptyDN	\$(UserID)@AcmeFinancial.com	No	No	No	No
<b>Title</b>	No	JobTitle		No	No	No	No
<b>Company</b>	No	CompanyName		No	No	No	No
<b>userAccountControl</b>	No	UserAccountControl	512	No	No	No	No
<b>Pager</b>	No	Pager		No	No	No	No
<b>Initials</b>	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
<b>RacfId</b>	Yes	RacfId		No	No	No	Yes
<b>Racfworkattrusename</b>	No	Racfworkattrusename		No	No	No	No
<b>UserBaseDn</b>	Yes	homeDirectory	profiletype=user, sysplex=sysplex1	No	No	No	No
<b>objectClass</b>	No	UserObjectClass	racfUser	No	No	No	No

Racfprogrammerna me	No	Racfprogrammerna me		No	No	No	No
Racfaddressline1	No	Racfaddressline1		No	No	No	No
Racfaddressline4	No	Racfaddressline4		No	No	No	No

## 618 2.1.24 External Provisioning Attributes

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

### 622 OPENLDAP

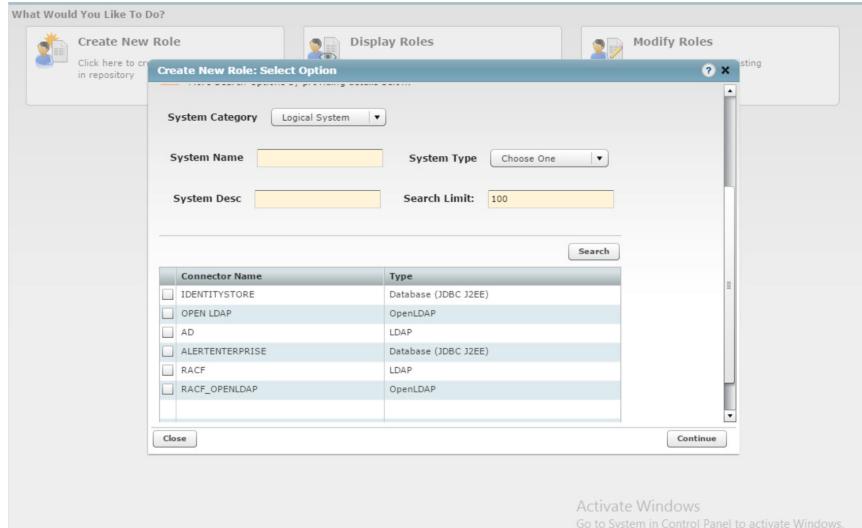
Name	Description
loginShell	loginShell

### 623 RACF\_OPENLDAP

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

## 624 2.1.25 Role Repository

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



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

631

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

**Create New Resource Role**

Follow the steps below to create Resource Role

Mandatory fields

**Details**

\* Role Name: [Input Field]  
Description: [Input Field]  
Resource Type: LDAP,OpenLDAP  
Resource(s): AD, OPEN LDAP

**Steps**

1 Attributes (Current Step) 2 Process 3 Owners 4 Risk  
5 Certification

Previous Step Next Step

**Attributes**

Role Comments Ma... Team Rooms:  
RoleHexCode: Functional Area:  
\*Alias: Location:  
Criticality: Process:  
Long Description: Alias1: Go to System in Control Panel to activate Windows.

632

633

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

\* Alias: Location:  
Criticality: Process:  
Long Description: Alias1:  
Status: Sub Process:  
EvaluateForOthers: Role Comments Ma...  
Role Comments Ma... Admin Full Name:  
Keywords: Technical Role Na...  
UME User Group: Role Stage:  
Role Sub Type:

Active for Provisioning: Yes Provisioning Assigned: Yes

Previous Step Next Step

634

635

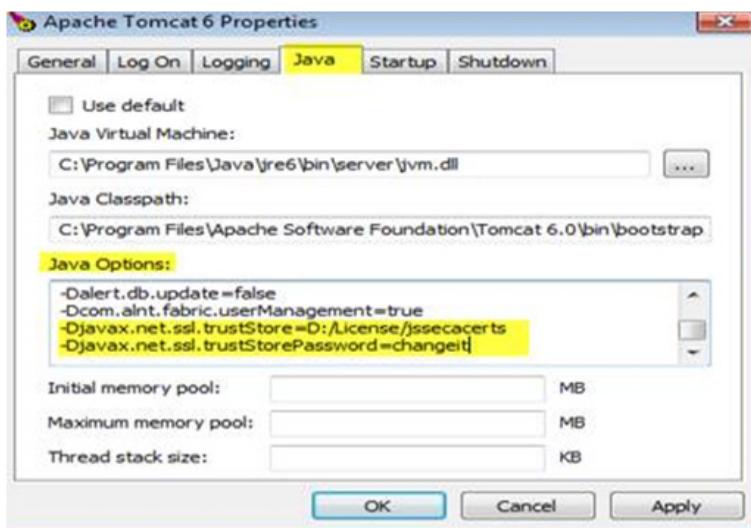
8. Create the following roles in the repository:

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

### 636 2.1.26 Enabling SSL

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

- 641 1. Create a *D:\cert\folder* on your system.
- 642 2. Place certificate jar file inside that folder.
- 643 3. Open the command prompt in administrator mode and perform the command:  
`cd D:\cert\`
- 645 4. Download certificate from directory server using the following command:  
`java -cp ALNTADCertUtil.jar com.alnt.ADCertInstaller <IP_Address_Of_Directory_Server>:636`
- 648 This creates the jssecacerts file in *D:\cert\* folder.
- 649 5. Add the following D parameters in <Tomcat Installation Folder>/bin/Tomact6w  
`-Djavax.net.ssl.trustStore=D:/License/jssecacerts`  
`-Djavax.net.ssl.trustStorePassword=changeit`



- 652
- 653 6. Copy jssecacerts to *D:/License* (create this folder if it does not exist) and restart Tomcat.
  - 654 7. Switch connection back to 636 port and set SSL as true from false.

## 655 2.2 HyTrust Cloud Control

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

### 661 2.2.1 How Its Used

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

## 664 2.2.2 Virtual Machine Configuration

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

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

670 VCenter Server:

- 671     ■ Windows Server 2012 R2
- 672     ■ 2 CPU core
- 673     ■ 16GB of RAM (memory)
- 674     ■ 1 NIC
- 675     ■ 60GB of storage

676 HTCC:

- 677     ■ CentOS 4/5/6/7 (64-bit)
- 678     ■ 4 CPU core
- 679     ■ 16GB of RAM (memory)
- 680     ■ 1 NIC
- 681     ■ 70GB of storage

### 682 Network Configuration (VCenter Server)

683 IPv4 Manual  
684 IPv6 Disabled  
685 IP Address: 192.168.20.6  
686 Netmask: 255.255.255.0  
687 Gateway: 192.168.20.1  
688 DNS Name Servers: 192.168.19.10  
689 DNS-Search Domains: acmefinancial.com

### 690 Network Configuration (HTCC)

691 IPv4 Manual  
692 IPv6 Disabled  
693 IP Address: 192.168.20.11  
694 Netmask: 255.255.255.0  
695 Gateway: 192.168.20.1  
696 DNS Name Servers 192.168.19.10  
697 DNS-Search Domains: acmefinancial.com

## 698 2.2.3 Installing Vcenter Server

699 Install Vcenter Sever 6.0 according to the VMware documentation found [here](#).

700 **2.2.4 Configuring Vcenter Server**

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

702 ESXi Host:

- 703 1. VMware ESXi, 6.0.0
- 704 2. Dell PowerEdge R620
- 705 3. 20 CPUs x 2.8 GHz
- 706 4. 23,478 mb / 262,098 mb
- 707 5. 8 Physical Adapters

708 **2.2.5 Deploying HTCC**

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

- 710 ▪ Virtual infrastructure, consisting of installed vCenter Servers and, optionally, ESX hosts.
- 711 ▪ Network connectivity and access to the HTCC host machine.
- 712 ▪ The HTCC installation requires an ESX host with at least one dedicated network interface (using VLANs).
- 713 ▪ 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*.
- 714 ▪ Services used by virtual infrastructure clients should be routable from the appropriate interface.

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

720 **2.2.6 Configuring HTCC**

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

723 **Configure the HTCC Management network interface:**

- 724 1. At the vSphere Client console window, log in as the user *ascadminuser* with the password  
Pa\$\$w0rd123!.
- 726 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.
- 728 3. Start the setup procedure. At the prompt, type: `setup`
- 729 4. Manually assign a static IP address to the management network interface (eth0) and set the  
subnet mask, gateway, and DNS server addresses.

- 731        5. Save by typing: y
- 732        6. Log out after network settings have been saved. This build is configured with the following  
733        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
```

- 734
- 735        The HTCC web-based management console is used to customize the HTCC settings. When accessing  
736        HTCC for the first time, you must use the IP address in the URL. For example:  
737        <https://<ipaddress>/asc>

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

- 740        The login screen appears.

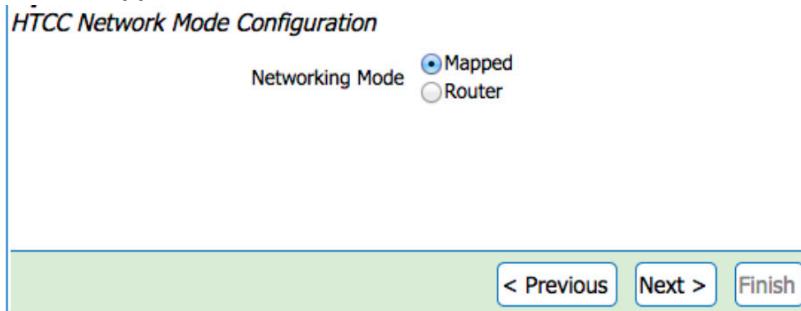
The screenshot shows a login interface with a blue header bar containing the word 'Login'. Below the header, there are two input fields: 'Username' and 'Password', both with placeholder text. At the bottom right of the form is a blue 'Login' button.

- 741
- 742        Once logged in, you can complete the initial setup and configuration. Here is an overview of the initial  
743        setup and configuration steps. The detailed steps can be found in the HTCC installation guide, which is  
744        available on request.

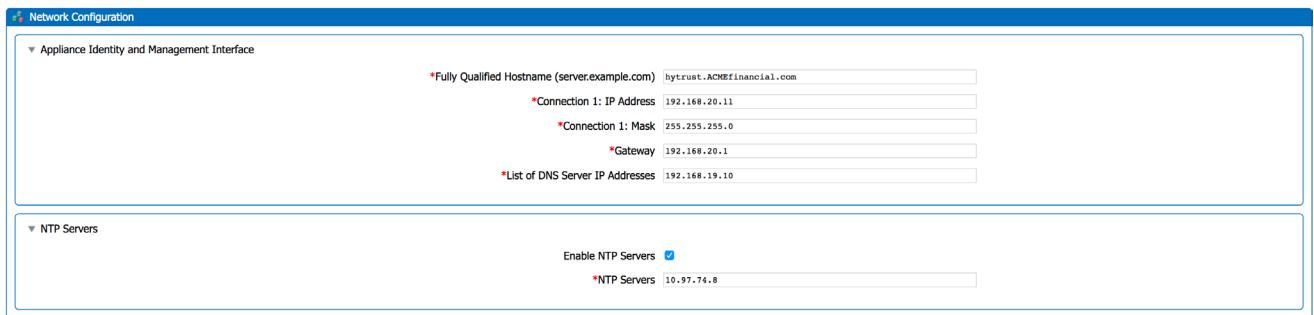
- 745        1. Accept the end-user license agreement.  
746        2. If applicable, install a license.  
747        3. Complete the **HTCC Installation Wizard** based on your selected networking mode.  
748        4. Perform post-installation setup.

- 749        **HTCC Installation Wizard:**

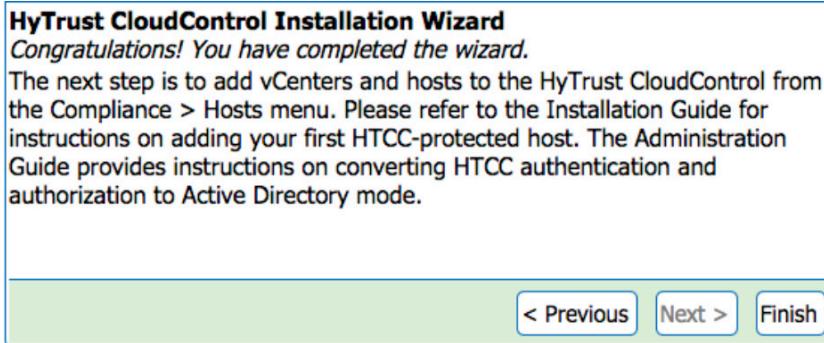
- 750 1. Select **Mapped** as the HTCC Network Mode



- 751  
752 2. Specify the network information on the Network Configuration page. This build is configured as  
753 follows:



- 754  
755 3. Click **Next** and select **Finish**.



- 756 < Previous Next > Finish

## 757 Add VCenter and Hosts to the HTCC:

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

Compliance > Hosts						
Type	Host Type	Patch Level	Label	Last Run Template	Last Run	Compliance
All	ESXi Host	VMware ESXi 6.0.0 build-3029758	N/A	Never	0%	
192.168.20.12	vCenter	6.0.0 build-3634793	N/A	N/A	N/A	
192.168.20.6	vSphere Web Client Server		N/A	N/A	N/A	

- 761

- 762 ESXi:

## DRAFT

763

\*Friendly Name

Description

\*Hostname/IP

Host Type

Protected

Managed

Labels

NONE
CoreAppliance
DEV
FirewallVM
HIPAA
INFRASTRUCTURE
MONITORING
PCI

Root Password Vaulting

\*SSH Port

Use VI SDK Secure Port

\*VI SDK Secure Port

Logging Aggregation

Local

Explicit Syslog Server

Syslog Server

764

765 Note: Ensure that each host is protected.

Published Hostname/IP

Published IP Mask

766

767 vCenter:

DRAFT

\*Friendly Name 192.168.20.6  
Description  
\*Hostname/IP 192.168.20.6  
User ID htaserviceaccount@acmefinancial.com  
Password \*\*\*\*  
Host Type vCenter  
Protected

768

\*HTTPS Secure Port 443  
Use HTTPS Secure Port   
\*HTTP Port 80  
Use VI SDK Secure Port   
\*VI SDK Port 80  
\*VI SDK Secure Port 443  
Logging Aggregation  Local  
 Explicit Syslog Server  
Syslog Server

Authentication Mode  Use HTCC Service Account (default)

769

Use of a Service Account is the only authentication mode currently supported with vSphere 6.

\*Published Hostname/IP 192.168.20.7  
\*Published IP Mask 255.255.255.0

770

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

773 vSphere Web Client Server:

\*Friendly Name

Description

\*Hostname/IP

User ID

Password

Host Type

Protected

Managed

774

Logging Aggregation  Local  
 Explicit Syslog Server

Syslog Server

Authentication Mode settings will be applied to all vCenters when connecting through this Web Client Server.

Authentication Mode  Use HTCC Service Account (default)

Use of a Service Account is the only authentication mode currently supported with vSphere 6.

775

\*Published Hostname/IP

\*Published IP Mask

776

## 2.2.7 Integrating With Active Directory

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

First, you must create a service account in Active Directory with the following permissions. In this build, 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**).

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

*Configuration > Authentication Configuration*

The screenshot shows the 'Authentication Configuration' page. At the top, there is a section titled 'Authentication Server Type' with two radio buttons: 'Demo' (unchecked) and 'Directory Service' (checked). Below this is a large green button labeled 'Apply'.

- 788  
789    The Active Directory Conversion Wizard opens, which guides you through the steps to connect HTCC  
790    to your directory service. The first page is the Configure Service Account page.

The screenshot shows the 'Active Directory Conversion Wizard - Configure Service Account' page. It includes sections for 'Domain' (Default Domain Name: acmefinancial.com), 'Service Account' (SSL Enabled: unchecked, Service Account Name: htcserviceaccount@acmefinancial.com, Service Account Password: four dots, Confirm Service Account Password: four dots), and 'Configuration Methods' (Automated Discovery selected). There is also a note: 'This Wizard will map Appliance roles to Active Directory groups in order to enforce authorization and policy.'

- 791  
792    3. Use the Service Account panel to specify the AD HTCC service account information. Select **Auto-**  
793    **mated Discovery**. Click **Next**.

- 794    Check **View Active Directory Advanced Settings** to view advanced settings. Otherwise, select **Next**.  
795

The screenshot shows the 'Available Domains' section of the Active Directory Advanced Settings page. It lists one domain: 'AcmeFinancial.com'. Below it is a section for 'Advanced Settings' with a checkbox labeled 'View Active Directory Advanced Settings' checked.

- 797    The Rule Conversion page appears where you can map HTCC roles to AD groups. For this build, we  
798    mapped the ASC\_SuperAdmin role to the Enterprise Admins Group.

The screenshot shows the 'Rule Conversion' page. It displays a table mapping HTCC roles to Active Directory groups. The rows are: 'ASC\_StorageAdmin' (AcmeFinancial), 'ASC\_SuperAdmin' (AcmeFinancial), and 'ASC\_ThirdParty' (AcmeFinancial). The 'Enterprise Admins' group is listed under the 'Active Directory Groups' column. At the bottom are buttons for 'Cancel', '< Previous', 'Next >', and 'Finish'.

- 800    Note: At a minimum, one Active Directory security group (e.g., SuperAdmin) must be mapped to HTCC  
801    ASC\_SuperAdmin role for AD conversion to be successful.

- 802    4. Click **Next**.

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

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

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

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

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

## 812 2.2.8 Creating and Deploying Access Policies

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

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

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

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

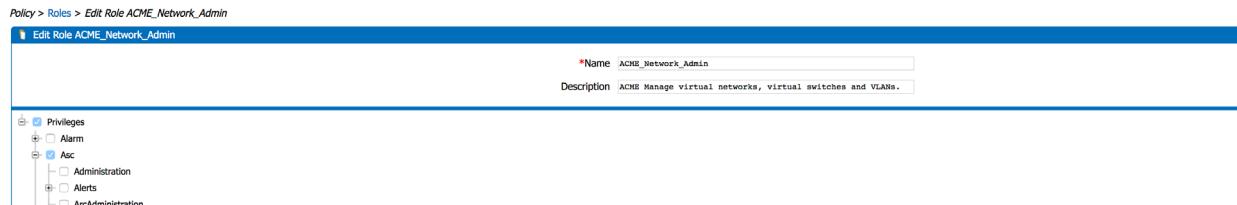
- 823 1. Open any **Policy** page.
- 824 2. Click the **Create Draft** button. This copies the "Deployed" policy to a "Draft" policy.
- 825 3. Make your desired changes to the Draft policy using the various policy pages.
- 826 4. Click the **Deploy** button to replace the current Deployed policy with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

827 For this build, two roles are created called **ACME\_Network\_Admin** and **ACME\_Systems\_Admin**. To cre-  
828 ate the rules and roles used to demonstrate the access rights management capability, follow these  
829 steps:

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

Name	Description
192.168.20.6.Admin	Full access rights
192.168.20.6.Anonymous	Not logged-in user (cannot be granted)

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



- 834  
835     4. Select all of the following permissions:
- 836         a. **Asc>NxOsConfig, NxOsShow, NxOsXmlApi,ssh,storage**  
837         b. **DVPortgroup>Entire List** (Note: This configuration item is deprecated in versions 5.1 and above of the product.)  
838         c. **DVSwitch>Entire List**  
839         d. **DataCenter>IpPoolConfig,IpPoolQueryAllocations,IpPoolReleaseIp**  
840         e. **Global>CancelTask,LogEvent**  
841         f. **Host>Config>AdvancedConfig,NetService,Network,PciPassthru**  
842         g. **Network>Assign,Delete,Router**  
843         h. **Resource>Delete**  
844         i. **System>Entire List**  
845         j. **Task>Entire List**  
846         k. **VirtualMachine>Config>ManagedBy,MultiActions**
- 847  
848     5. Press **OK**.  
849     6. Press **Deploy**.  
850     7. Repeat Steps 2–6 to create the system admin role, but with the following permissions selected:
- 851         a. **Global>CancelTask,LogEvent**  
852         b. **System>Entire List**  
853         c. **Task>Entire List**  
854         d. **VApp>Entire List**  
855         e. **VirtualMachine>Entire List**

856 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.

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

Rules			
Monitor Only	Policy	Deployed	
<input type="checkbox"/>	<input type="text"/> Search:	<input type="button" value="Go"/>	
<input type="button" value="Add"/>	<input type="button" value="Delete"/>	<input type="button" value="Copy"/>	<input type="button" value="Assign"/>
<input type="button" value="Create Draft"/>	<input type="button" value="Discard Changes"/>	<input type="button" value="Deploy"/>	
Showing 1 to 32 of 32		Show: 10 20 50 100 200 500	Pages: << < > >>
Name	Domain User Group	Role	Description
Acme_VMRule	acmefinancial\HyTrust Users	ACME_Systems_Admin	ACME
VIRTUAL_CENTER_VSPHERE.LOCAL\Administrators	VSPHERE.LOCAL\Administrators	192.168.20.6.Admin	Default rule for VIRTUAL_CENTER_VSPHERE.LOCAL\Administrators
VIRTUAL_CENTER_VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator	192.168.20.6.Admin	Default rule for VIRTUAL_CENTER_VSPHERE.LOCAL\Administrator
VIRTUAL_CENTER_VSPHERE.LOCAL\pxd-b1ba5910-6569-11e6-102-168-20-6	VSPHERE.LOCAL\pxd-b1ba5910-6569-11e6-102-168-20-6	192.168.20.6.Admin	Default rule for VIRTUAL_CENTER_VSPHERE.LOCAL\pxd-b1ba5910-6569-11e6-102-168-20-6

- 860  
861     10. Select **Add**. Name the rule and type in the user group created in Active Directory.

Policy > Rules > Edit Rule Acme\_VM\_Rule

**Edit Rule Acme\_VM\_Rule**

Name: <input type="text" value="Acme_VM_Rule"/>	Domain: <input type="text" value="acmefinancial"/>										
User Group: <input type="text" value="HyTrust Users"/>	Role: <input type="text" value="ACME_Systems_Admin"/>										
Propagate: <input checked="" type="checkbox"/>	Description: <input type="text" value="ACME"/>										
Assign to Policy Resource <input type="button" value="Assign"/>											
<b>Constraints</b>											
<table border="1"> <thead> <tr> <th>Add</th> <th>Delete</th> </tr> </thead> <tbody> <tr> <td>Show 0 to 0 of 0</td> <td></td> </tr> <tr> <td><input type="button" value="Edit"/></td> <td><input type="button" value="Constraint Type"/></td> </tr> <tr> <td colspan="2">No Records Found</td> </tr> <tr> <td colspan="2">Show: 10 20 50 100 200 500 Pages: &lt;&lt; &lt; &gt; &gt;&gt;</td> </tr> </tbody> </table>		Add	Delete	Show 0 to 0 of 0		<input type="button" value="Edit"/>	<input type="button" value="Constraint Type"/>	No Records Found		Show: 10 20 50 100 200 500 Pages: << < > >>	
Add	Delete										
Show 0 to 0 of 0											
<input type="button" value="Edit"/>	<input type="button" value="Constraint Type"/>										
No Records Found											
Show: 10 20 50 100 200 500 Pages: << < > >>											
<b>Assigned Resources</b>											
<table border="1"> <thead> <tr> <th>Showing 1 to 2 of 2</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input type="button" value="Edit"/></td> <td>Folder:group-d1 @ https://192.168.20.6:443/sdk</td> </tr> <tr> <td>No Records Found</td> <td></td> </tr> <tr> <td colspan="2">Show: 10 20 50 100 200 500 Pages: &lt;&lt; &lt; &gt; &gt;&gt;</td> </tr> </tbody> </table>		Showing 1 to 2 of 2	Description	<input type="button" value="Edit"/>	Folder:group-d1 @ https://192.168.20.6:443/sdk	No Records Found		Show: 10 20 50 100 200 500 Pages: << < > >>			
Showing 1 to 2 of 2	Description										
<input type="button" value="Edit"/>	Folder:group-d1 @ https://192.168.20.6:443/sdk										
No Records Found											
Show: 10 20 50 100 200 500 Pages: << < > >>											
<b>Assigned RuleSets</b>											
<table border="1"> <thead> <tr> <th>Showing 0 to 0 of 0</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input type="button" value="Edit"/></td> <td></td> </tr> <tr> <td>No Records Found</td> <td></td> </tr> <tr> <td colspan="2">Show: 10 20 50 100 200 500 Pages: &lt;&lt; &lt; &gt; &gt;&gt;</td> </tr> </tbody> </table>		Showing 0 to 0 of 0	Description	<input type="button" value="Edit"/>		No Records Found		Show: 10 20 50 100 200 500 Pages: << < > >>			
Showing 0 to 0 of 0	Description										
<input type="button" value="Edit"/>											
No Records Found											
Show: 10 20 50 100 200 500 Pages: << < > >>											

862

### 11. Select **Assign**.

863

### 12. Check the **HyTrust CloudControl Appliance Root** radio button.

Policy > Rules > Edit Rule Acme\_VM\_Rule > Assign Rules to Policy Resources and RuleSets

**Assign Rules to Policy Resources and RuleSets**

You are assigning the following rules: Acme\_VM\_Rule

Search:  Go

Resources  RuleSets

Virtual Center  Host  Virtual Machine  Virtual Application  Portgroup  vSwitch

Network  DataCenter  Datastore  Cluster  Folder  Resource Pool

Network Service Container  DHCP  Load Balancer  VPN  IPSEC VPN  Router  Controller  Switch

Showing 1 to 20 of 29

Results	Current Rules	Current RuleSets
<input type="checkbox"/> Web Client	Rule(s): Default VMUser rule	
<input type="checkbox"/> Server 192.168.20.6	Rule(s): Default ARCAAdmin rule, Acme_VM_Rule2, Default SecurityAdmin rule, Default SecurityAuditor rule, Default RoleAdmin rule, Default UCS rule, Default DCAdmin rule, Default SuperAdmin rule, Default ThirdParty rule, Default KVMAAdmin rule, Acme_VM_Rule, Default ESXKAdmin rule, Default AppAdmin rule, Default NetworkEngineer rule, Default NetworkAdmin rule, Default CoreAppAdmin rule, Default PolicyAdmin rule, Default LoadBalancer rule, Default NetworkOperator rule, Default StorageAdmin rule, Default VMUser rule	
<input checked="" type="checkbox"/> HyTrust		
<input checked="" type="checkbox"/> CloudControl Appliance Root		

Show: 10 20 50 100 200 500 Pages: << < 1 2 > >>

864

### 13. Select **OK**.

865

### 14. Select **OK**.

866

### 15. Select **Deploy**.

867

### 16. Repeat Steps 1–9 to create a rule for the network admins role, assigning it to the '*Hytrust Users*' active directory group.

868

## 2.2.9 Configure Logging

869

### 1. Select **Configuration > Logging**.

870

### 2. Select the **DEBUG** logging level.

871

### 3. Select **External**.

872

### 4. Select **CEF**.

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

The screenshot shows the 'Logging Configuration' section of a software interface. It has two main sections: 'HTCC Logging Configuration' and 'Host Default Logging Configuration'. In the 'HTCC Logging Configuration' section, the 'Logging Level' is set to 'DEBUG'. Under 'HTCC Logging Aggregation', 'External' is selected over 'Local'. For 'Logging Aggregation Template Type', 'CEF' is selected over 'Proprietary'. The 'HTCC Syslog Servers' field contains the IP address '192.168.17.10:514'. Below it, there are buttons for 'Encrypt Syslog', 'Manage Logs' (with 'Download' and 'Reset' options), 'Repair Log' (with 'Repair' and 'Reset' options), and 'Log Viewer' (with 'Reset' option). In the 'Host Default Logging Configuration' section, 'Explicit Syslog Server' is selected over 'Local'. The 'Default Syslog Server' field also contains the IP address '192.168.17.10:514'. At the bottom right of the interface is a green 'Apply' button.

877  
878        6. Select **Explicit Syslog Server**.  
879        7. Enter the IP address of the Splunk server, specify port 514.  
880        8. Select **Apply**.

## 881      2.3 Microsoft Active Directory

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

### 883      2.3.1 How It's Used

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

### 889      2.3.2 Virtual Machine Configuration

890 The AD virtual machine is configured as follows:

- 891        ▪ 1 CPU Core
- 892        ▪ 4GB RAM
- 893        ▪ 84GB HDD
- 894        ▪ 2 Network Adapters

#### 895      Network Configuration (Interface 1)

- 896        IPv4 Manual
- 897        IPv6 Disabled
- 898        IP Address: 192.168.19.10
- 899        Netmask: 255.255.255.0
- 900        Gateway: 192.168.19.1

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

### 903 2.3.3 Installing AD

904 Install a new Windows server 2012 R2 Active Directory Forest:

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

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

### 908 2.3.4 DNS Configuration

- 909 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

- 910 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

### 911 2.3.5 Installing Splunk Universal Forwarder

912 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](https://www.splunk.com/page/sign_up)

914 Download the Splunk Universal Forwarder from: [http://www.splunk.com/en\\_us/download/universal-forwarder.html](http://www.splunk.com/en_us/download/universal-forwarder.html)

916 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

918 **2.3.6 Install Security Compliance Manager**

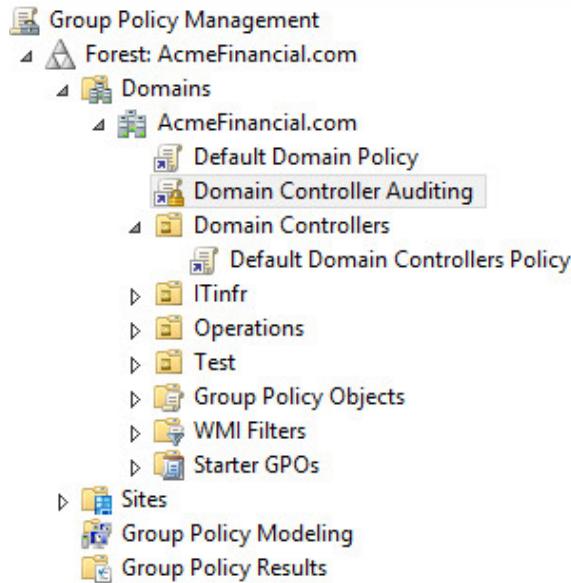
919 Install Microsoft Security Compliance Manager: [https://www.microsoft.com/en-](https://www.microsoft.com/en-us/download/details.aspx?id=53353)  
 920 [us/download/details.aspx?id=53353](https://www.microsoft.com/en-us/download/details.aspx?id=53353)

921 **2.3.7 Group Policy Object (GPO) Configuration**

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

925 SCM consist of baseline configurations based on Microsoft security guide recommendations and  
 926 industry best practices. In this build, the Domain Controller Security Policy is deployed using SCM to  
 927 established a benchmark. The .CAB file is included in the SCM. In our build, we deployed this benchmark  
 928 named as “Domain Controller Auditing.” For directions for deploying a benchmark, see the Microsoft  
 929 documentation found [here](#).

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



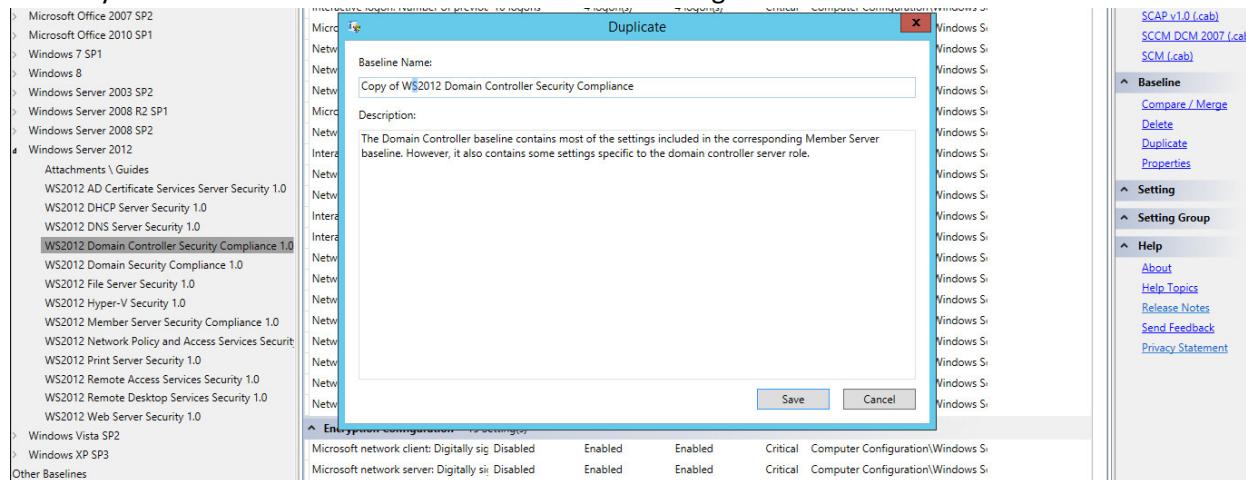
932

933 For this build, no changes are made to the Default Domain or Default Domain Controllers Policy. Both  
 934 policies are “enabled” and “link enabled.”

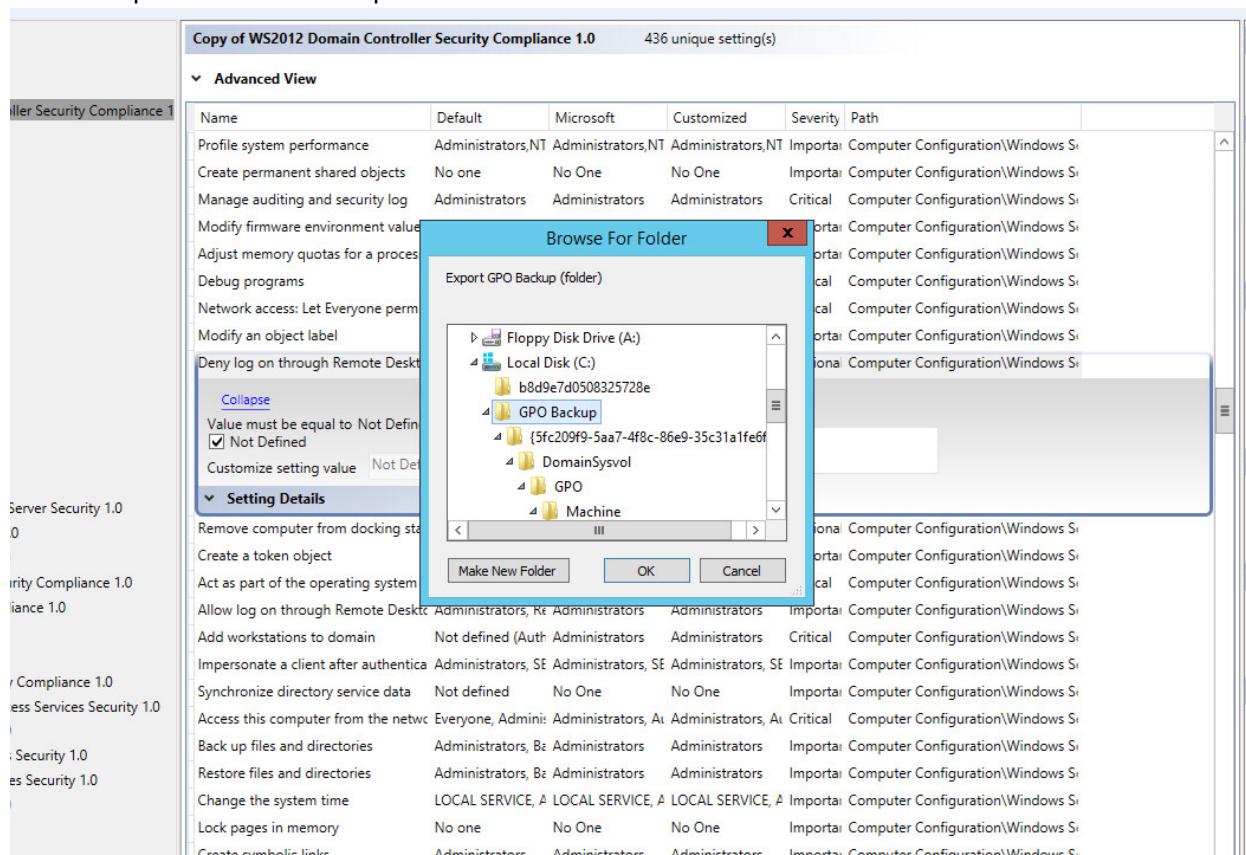
935 Minor changes are made to the Domain Controller Auditing Policy to enable the ability to audit user  
 936 account changes, attribute changes, and policy changes for this build.

937 *Note:* This example is built in a lab environment. Some security measures were dialed back or turned off  
 938 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.

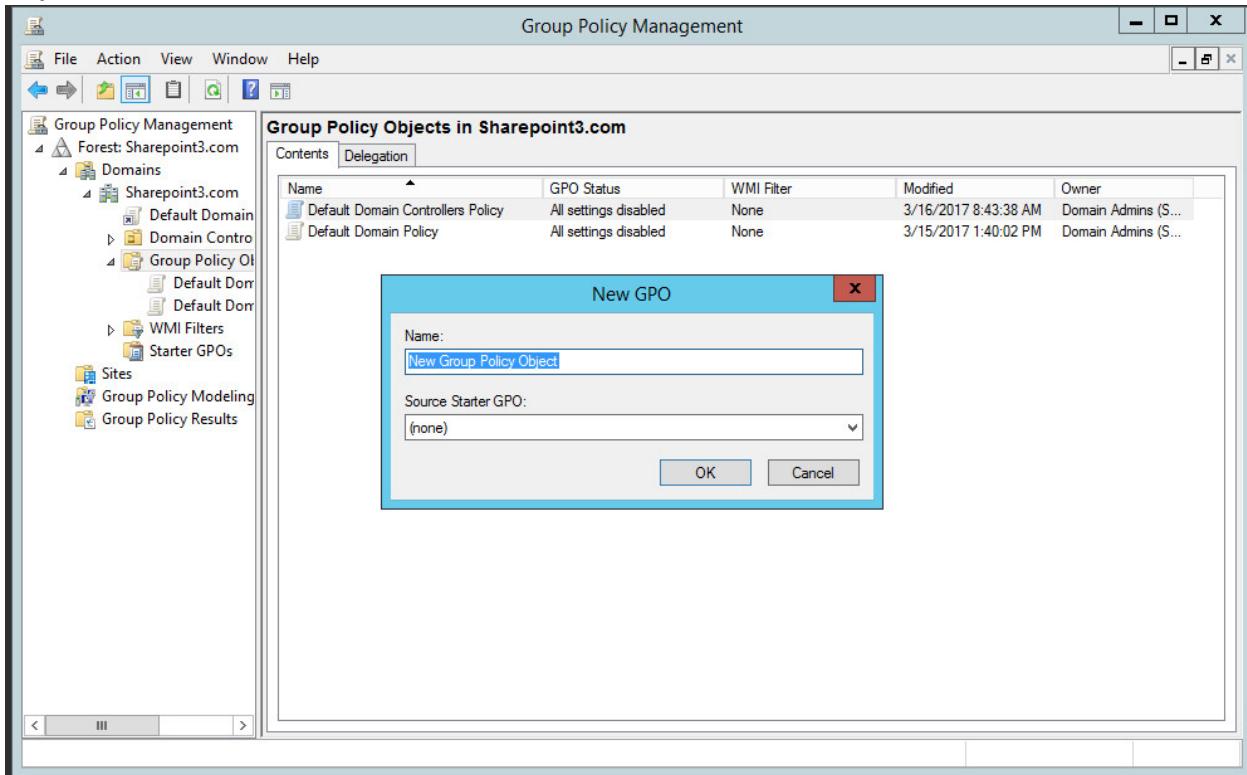


- 941      2. Export to a GPO backup folder.  
 942

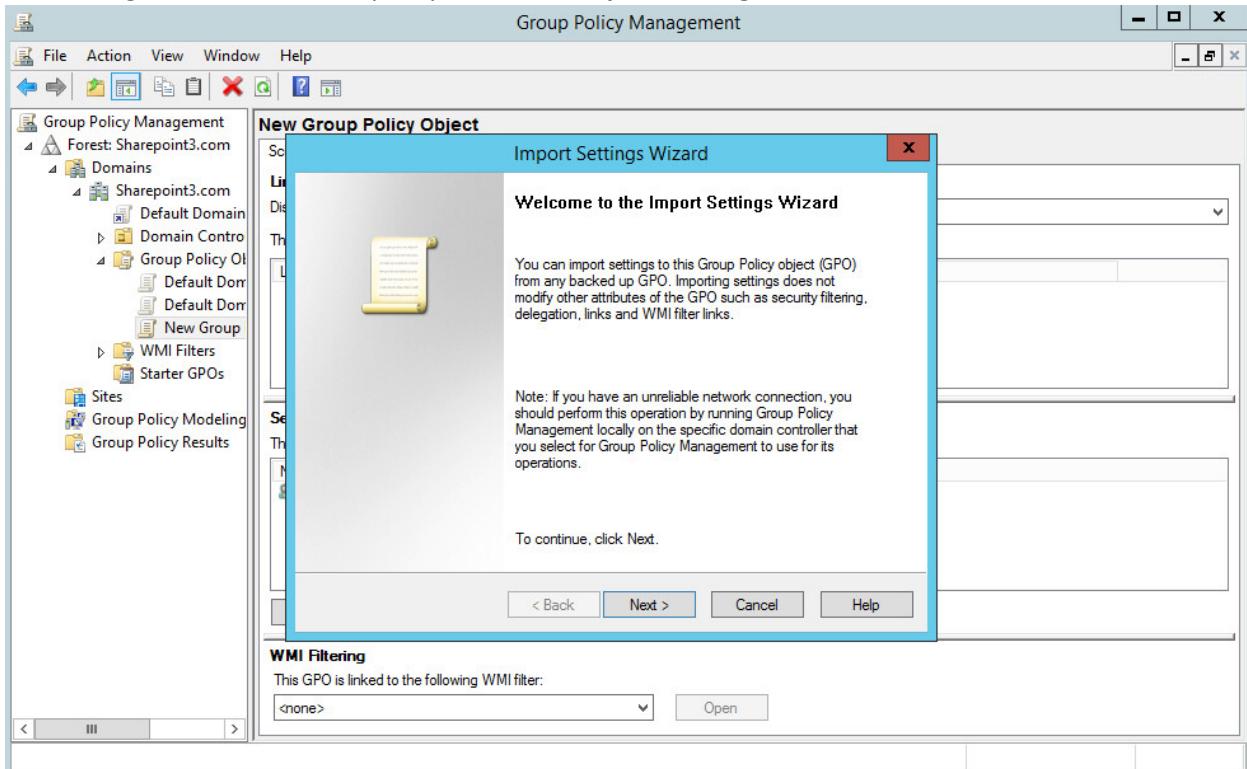


943

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



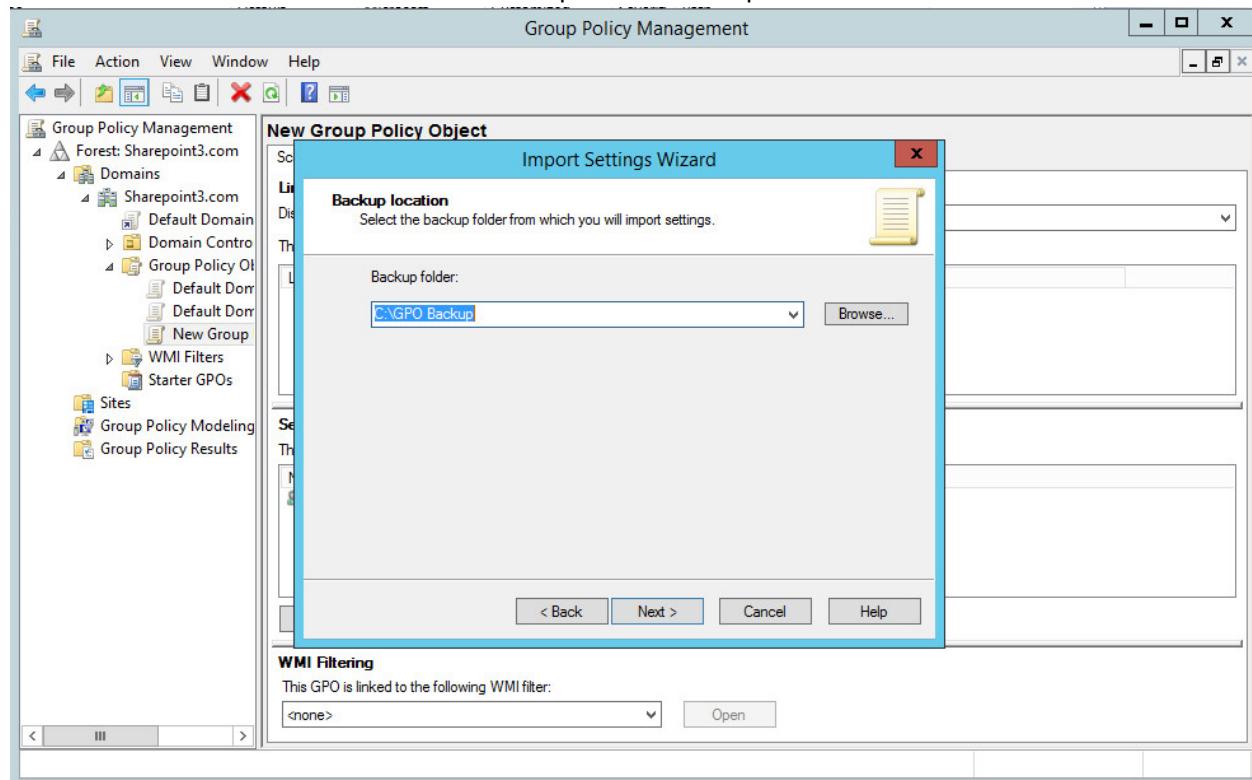
- 946  
947      4. Right-click on the new policy and select **Import Settings**. Click **Next**.



948

949

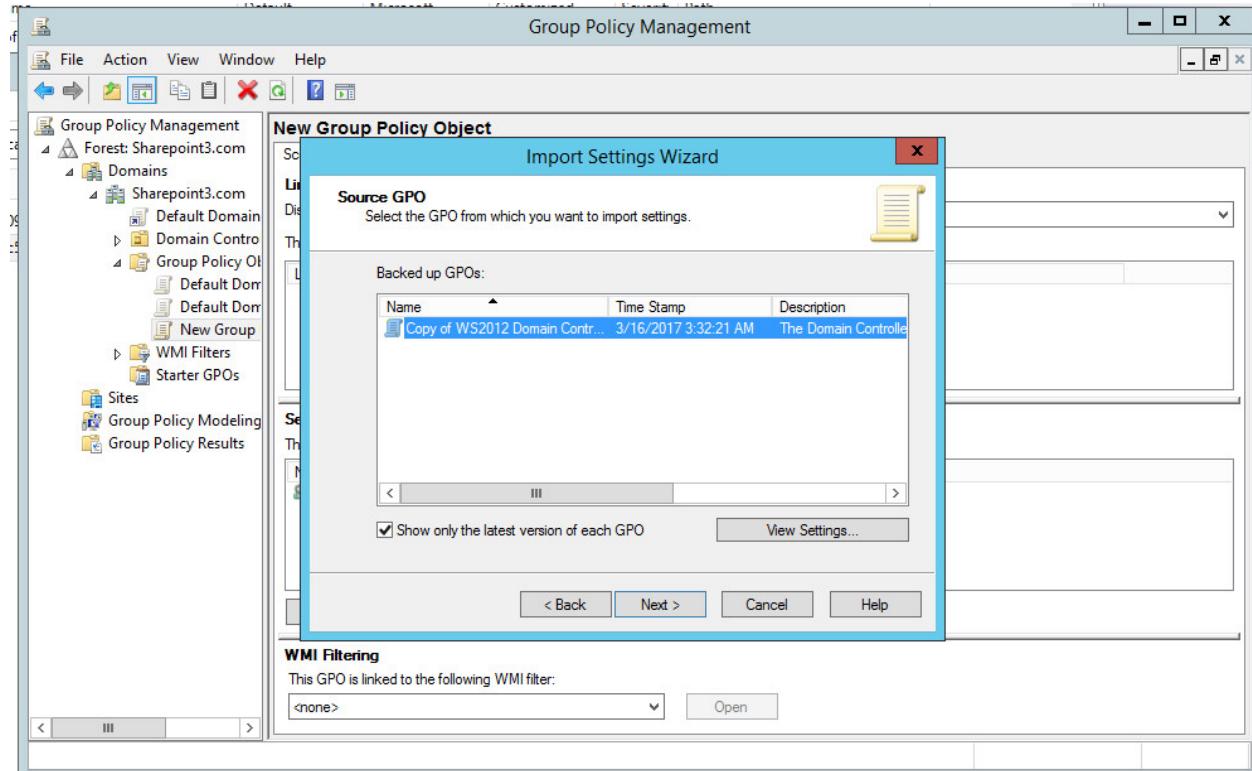
5. Select the folder location of the backup created in Step 2. Select **Next**.



950

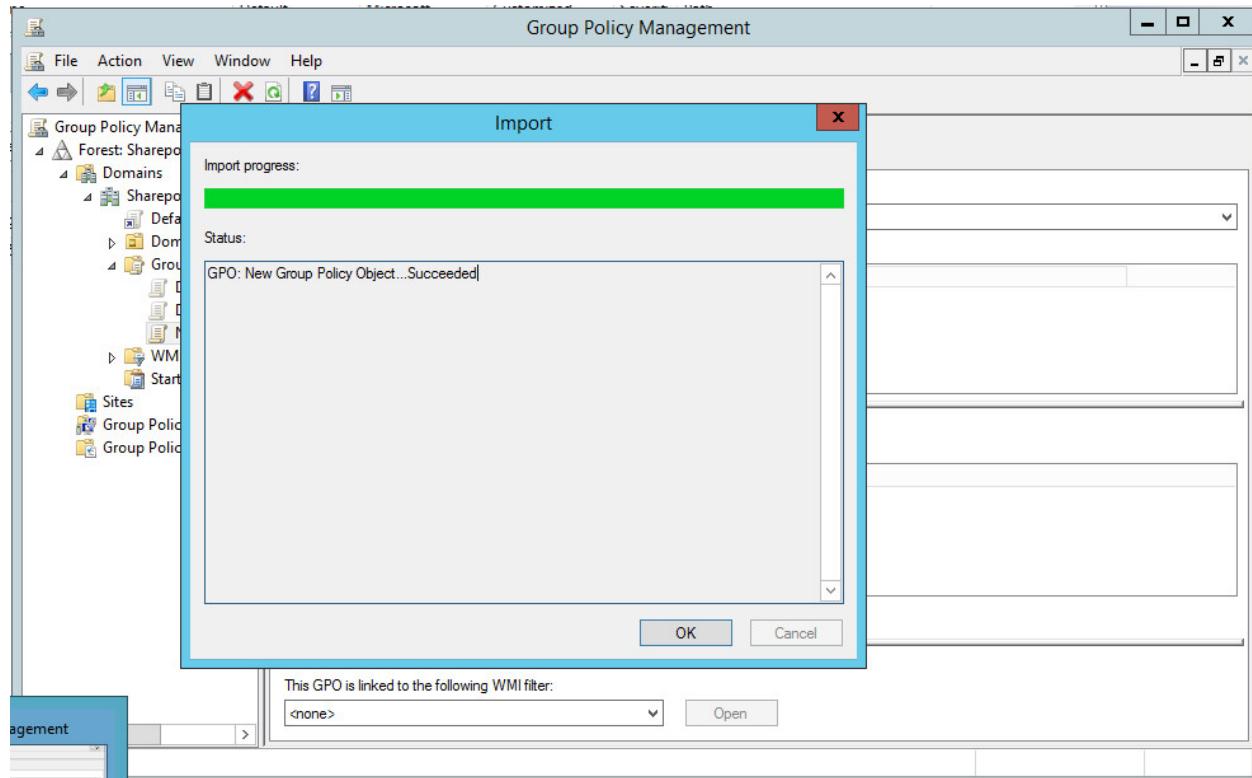
951

6. Select the backup created in Step 2.

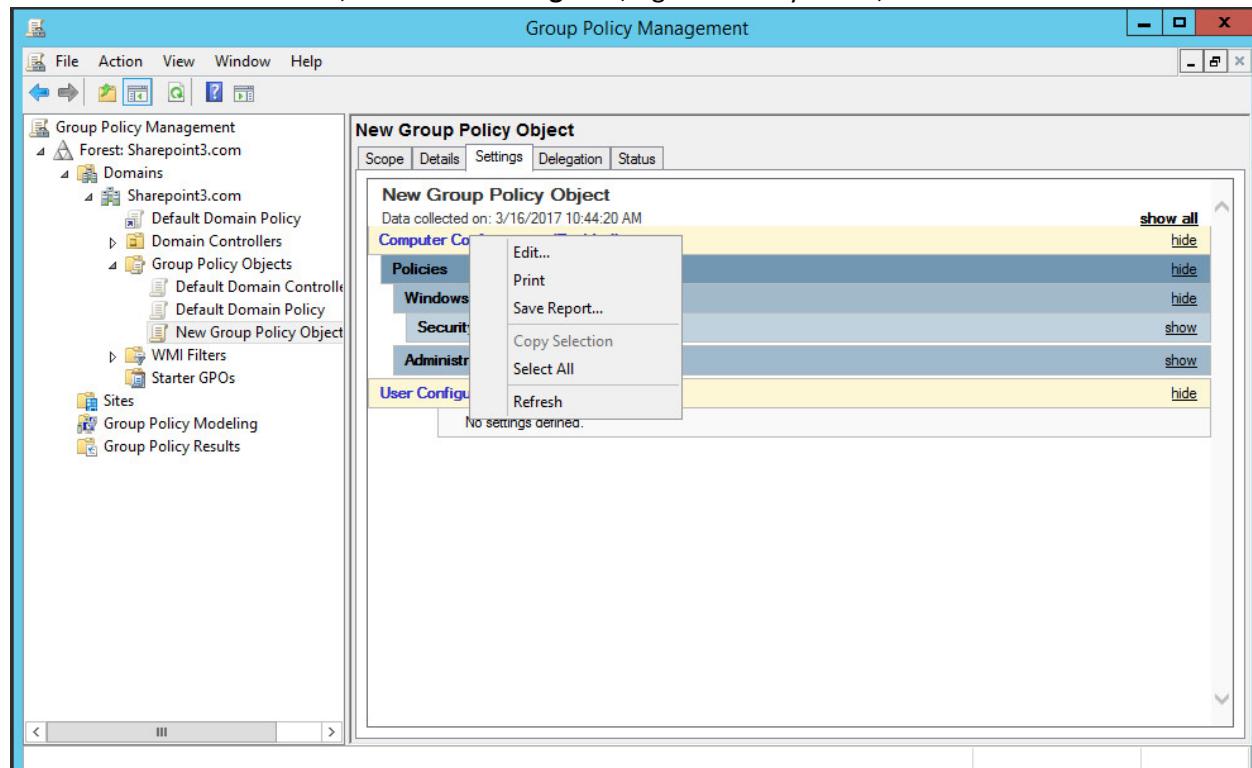


952

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

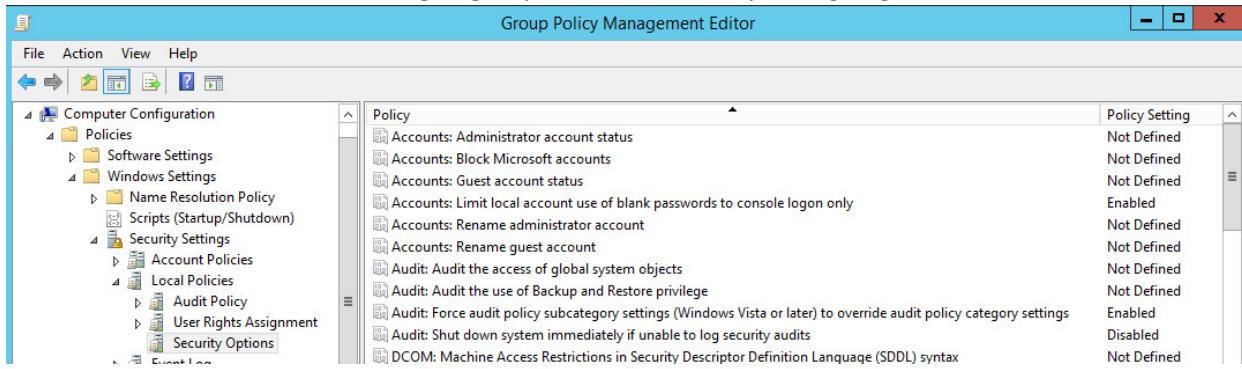


954  
955 8. Select the new GPO, select the **Settings** tab, right-click anywhere, and select **Edit**.



956  
957 9. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies>Security Options**. Change the value for "Audit: Force audit policy subcategory settings

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



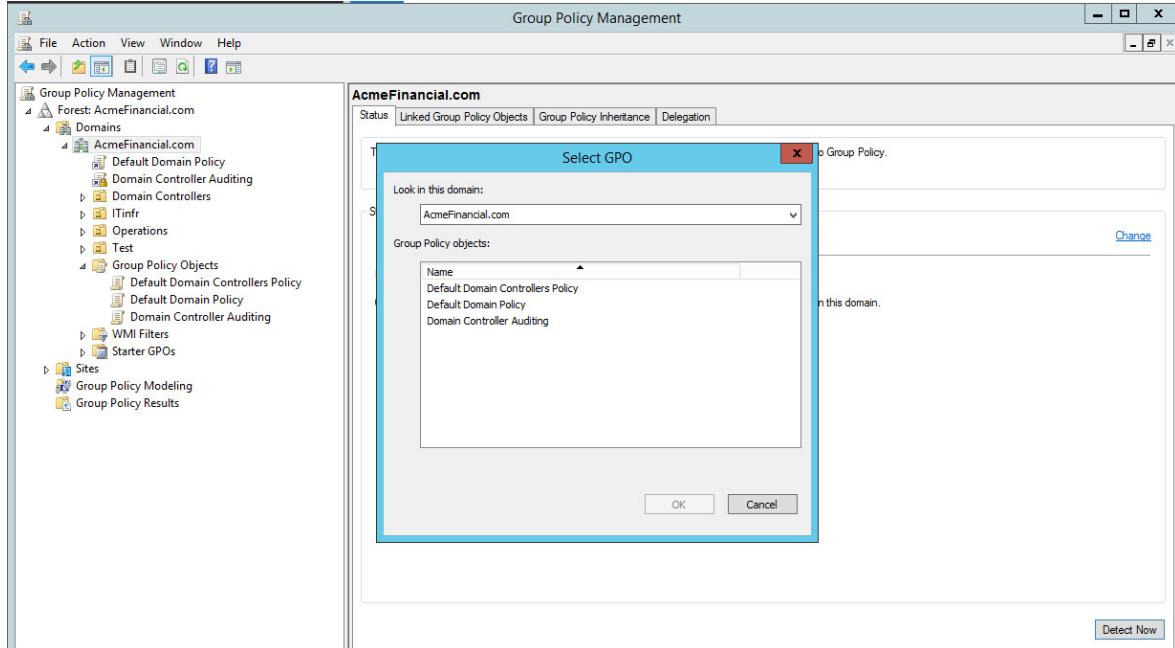
The screenshot shows the Group Policy Management Editor window. The left pane displays a tree structure under "Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies". The right pane lists various audit policies with their current "Policy Setting":

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Audit: Shut down system immediately if unable to log security audits	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not Defined

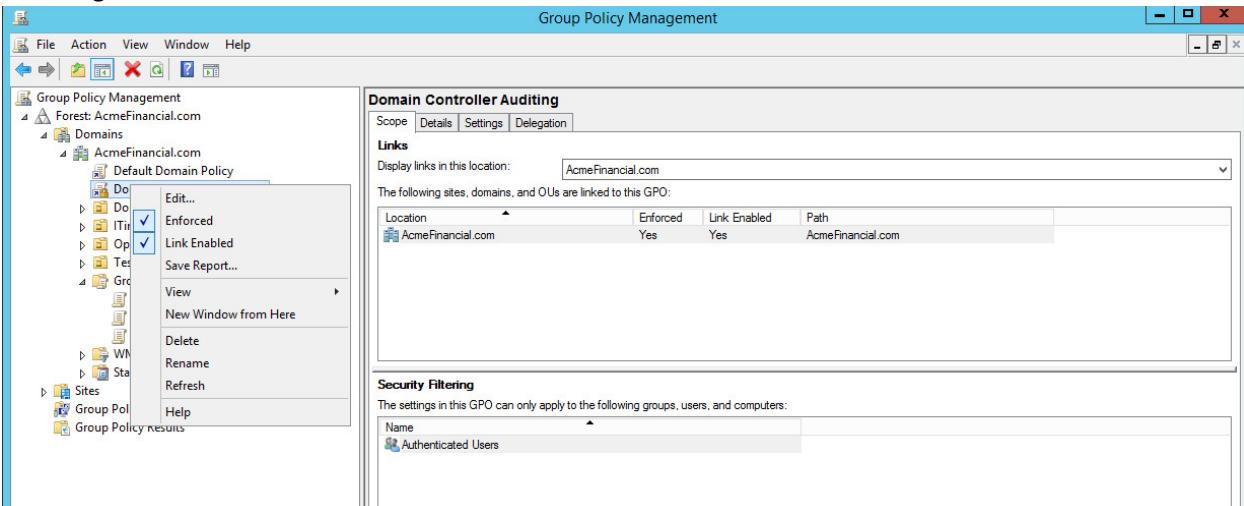
- 961  
 962 10. Navigate to Computer Configuration>Policies>Windows Settings>Security Settings>Advanced  
 963 Audit Policy Configuration>Audit Policies. Make the following changes and save:

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

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

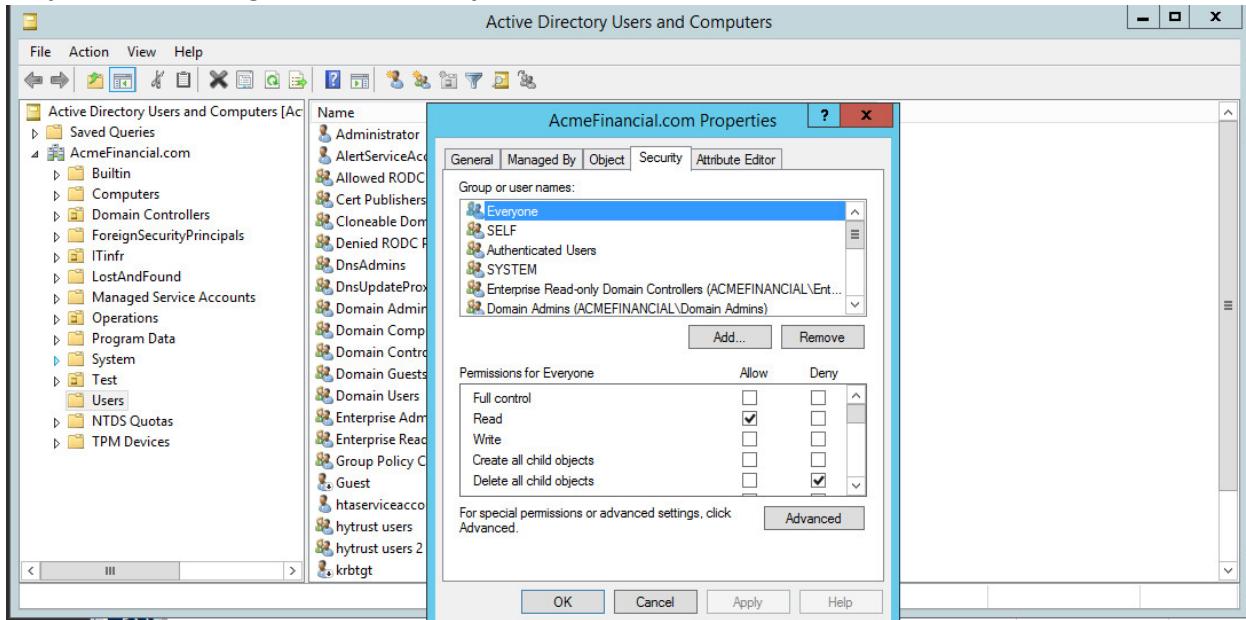


- 966        12. Right-click on the new GPO linked directly under the top-level domain and select **Enforced** by  
 967 checking it on the left.

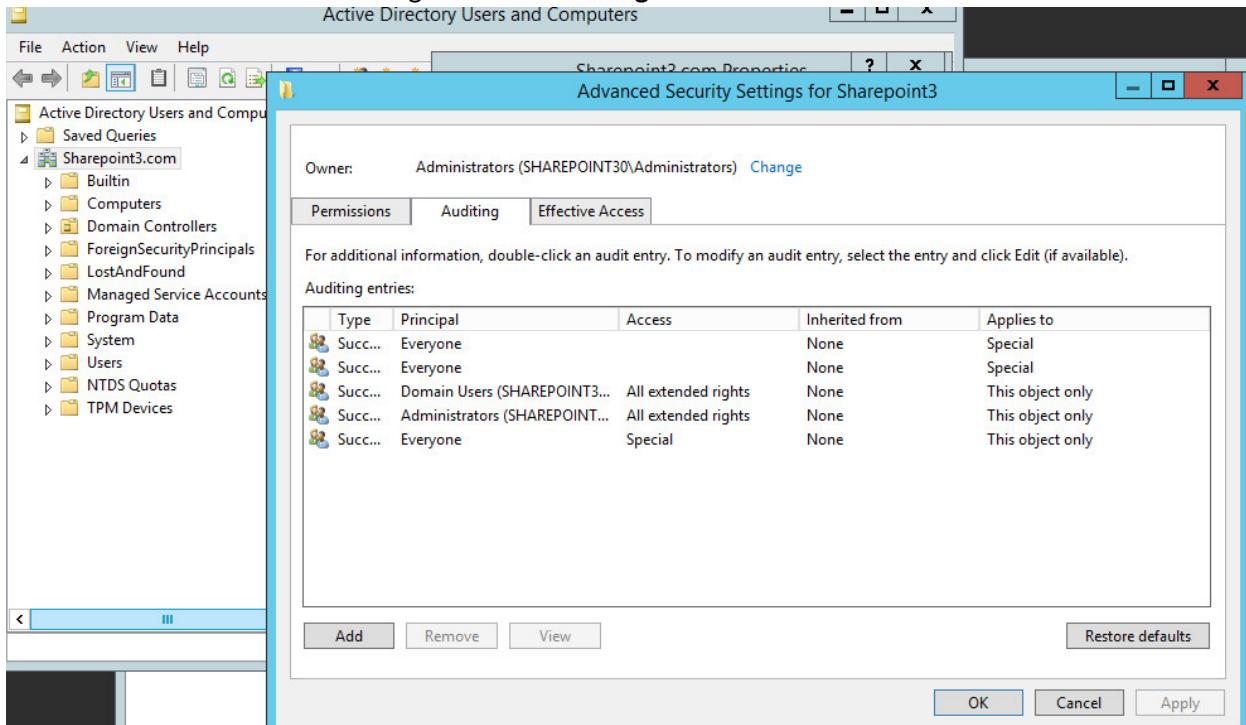


968

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

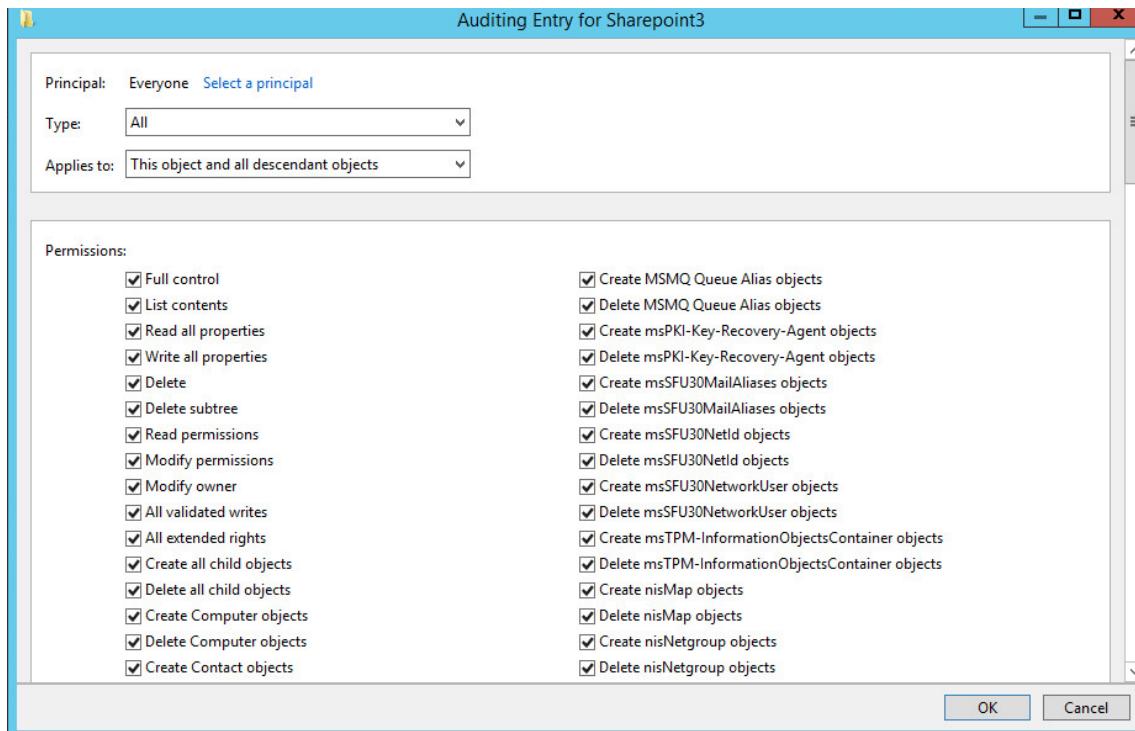


- 971      972      14. Select Advanced and navigate to the Auditing tab.



- 973      974      15. Add a new entry with the following parameters:

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



### 978 2.3.8 Script: AdDOnlineStatus.ps1

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

```
981 #This script determines if this server is online or offline
982 #If a gateway route exists, the script will
983 #output the current time, hostname, status and previous time (last
984 #time it wrote to output file)
985 #Check if gateway route exists
986 if (Get-Netroute 0.0.0.0/0)
987 {
988     #Store date in PrevTime variable
989     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
990     #Check if prevtime-file.txt exists
991     if (ls C:\scripts\prevtime-file.txt)
992     {
993         #Place the contents of prevtime-file.txt in the PrevTime variable
994         $PrevTime=Get-Content C:\scripts\prevtime-file.txt
```

```

995      }
996      #Place the current date in CurrentTime
997      $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
998      #Overwrite the contents of prevtime-file.txt with the current date
999      Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy" > C:\scripts\prevtime-file.txt
1000     $HostVar = hostname
1001     $Status = 'online'
1002     #Add the contents of the variables CurrentTime, HostVar, Status, PrevTime to
1003     Radiant-Status-Output.csv
1004     Add-Content C:\scripts\AD-Status-Output.csv
1005     $CurrentTime', '$HostVar', '$Status', '$PrevTime
1006   }
1007 else
1008 {
1009   $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1010   if (ls C:\scripts\prevtime-file.txt)
1011   {
1012     $PrevTime=Get-Content C:\scripts\prevtime-file.txt
1013   }
1014   $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1015   Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy" > C:\scripts\prevtime-file.txt
1016   $HostVar = hostname
1017   $Status = 'offline'
1018   Add-Content C:\scripts\AD-Status-Output.csv
1019   $CurrentTime', '$HostVar', '$Status', '$PrevTime
1020 }

```

### 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**.



- 1029  
1030 4. Click **Next**  
1031 5. Choose the placement of the certificate:  
1032     a. Choose to place the certificate in the **Personal Store** if it is the domain controller's  
1033         certificate.  
1034     b. Choose to place the certificate in the **Trusted Store** if it is the CA certificate.  
1035 6. Click **OK** and then click **Next**.  
1036 LDAPS requests can be processed at this point.



1037

## 2.4 NextLabs Entitlement Manager

1039 NextLabs Entitlement Manager is a dynamic authorization system based on Attribute Based Access  
1040 Control.

### 2.4.1 How It's Used

1042 NextLabs Entitlement Manager is used to authorize access to the web application, which is SharePoint in  
1043 this build. Entitlement Manager requires three components for functionality: NextLabs Control Center,  
1044 Policy Studio, and Entitlement Management for Microsoft SharePoint Server.

1045 NextLabs Control Center is installed on its own server along with Policy Studio. Entitlement  
1046 Management is installed on an instance of Microsoft SharePoint Server.

### 2.4.2 Virtual Machine Configuration

1048 The NextLabs virtual machine is configured with:

1049     ■ Windows Server 2012 R2

1050     ■ 8 CPU cores

1051     ■ 16GB of RAM

1052     ■ 1 NIC

1053     ▪ 100GB of Storage

1054 **Network Configuration (Interface 1)**

1055 IPv4 Manual

1056 IPv6 Disabled

1057 IP Address: 192.168.14.117

1058 Netmask: 255.255.255.0

1059 Gateway: 192.168.14.1

1060 DNS Name Servers: 192.168.14.1

1061 DNS-Search Domains: n/a

1062 **2.4.3 Prerequisites**

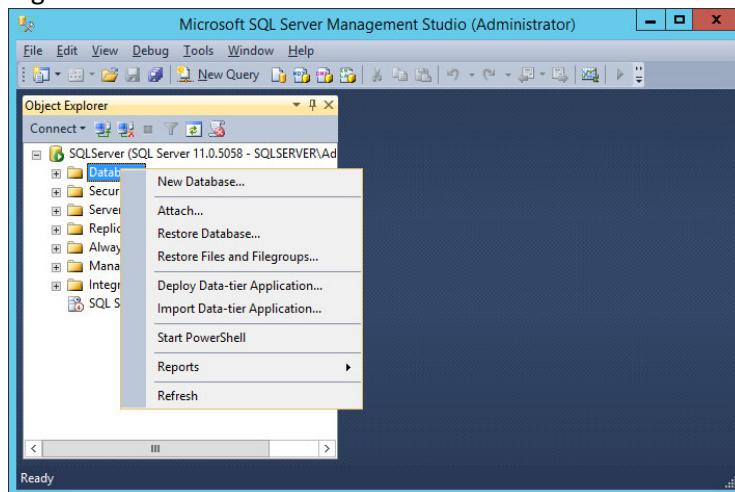
1063 NextLabs Control Center requires an Oracle or MS SQL Server. It is recommended that the database be  
1064 given 500GB of free storage space. In this build, only 100GB of storage is used for development  
1065 purposes.

1066 Additionally, multiple deployment configurations are supported. The development deployment  
1067 configuration is used in this build. For this deployment, the Control Center server is deployed on the  
1068 same instance as the SQL Server. For a full list of supported software and deployment configurations,  
1069 see the *NextLabs Control Center Installation Guide* found at the [customer portal](#).

1070 **2.4.4 Installing NextLabs**

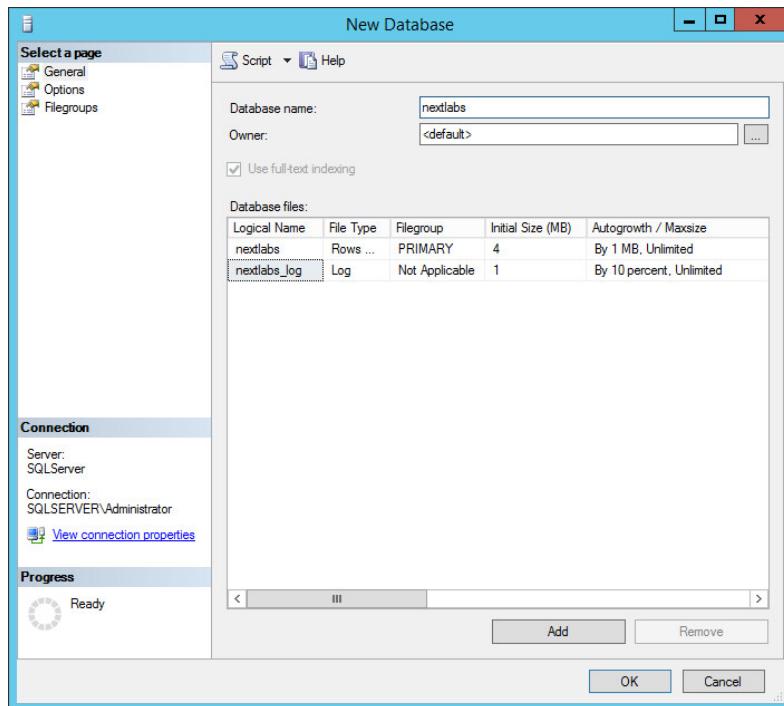
1071 **Control Center 7.7**

- 1072     1. Install the Microsoft SQL Server 2012 according to instructions available [online](#).
- 1073     2. Open Microsoft SQL Server Management Studio and log in to the Microsoft SQL Server.
- 1074     3. Right-click on **Databases** and left-click on **New Database**.



- 1075     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

1078

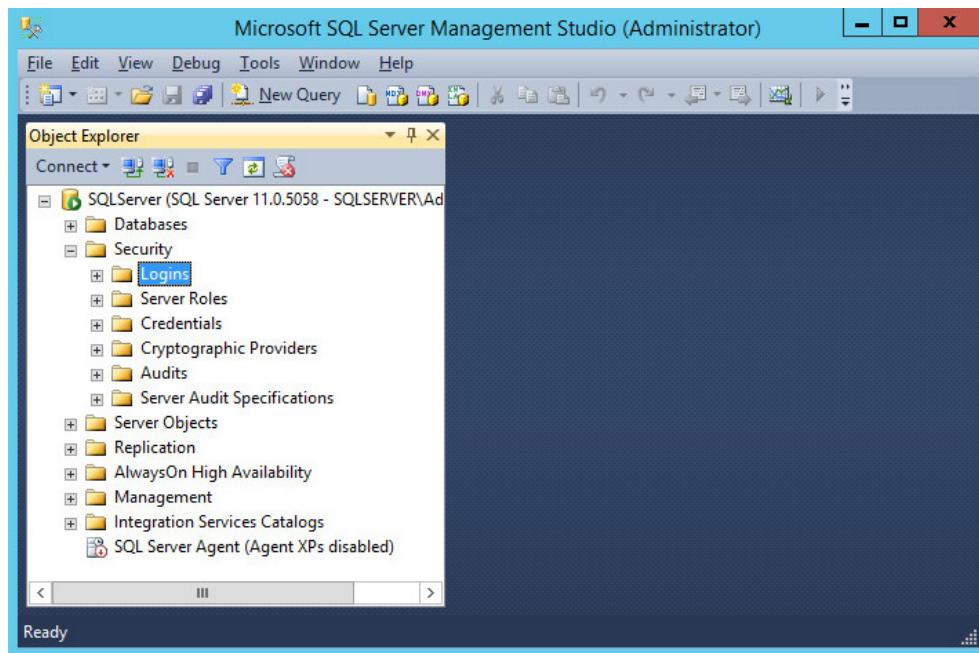
from this build: **nextlabs**.

1079

1080

1081

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.

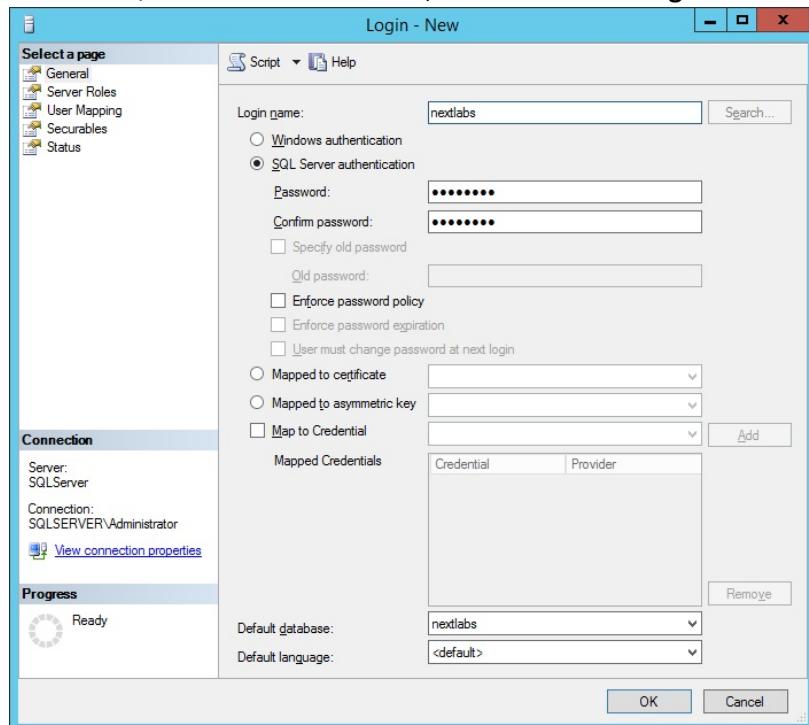


1082

1083

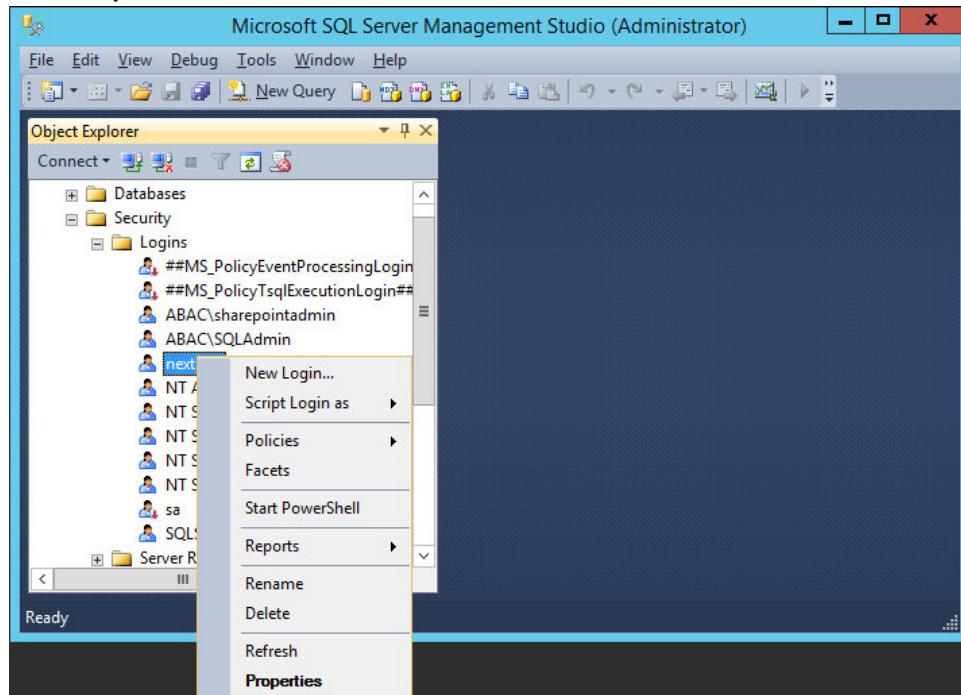
6. Right-click **Logins**. Left-click **New Login**.

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



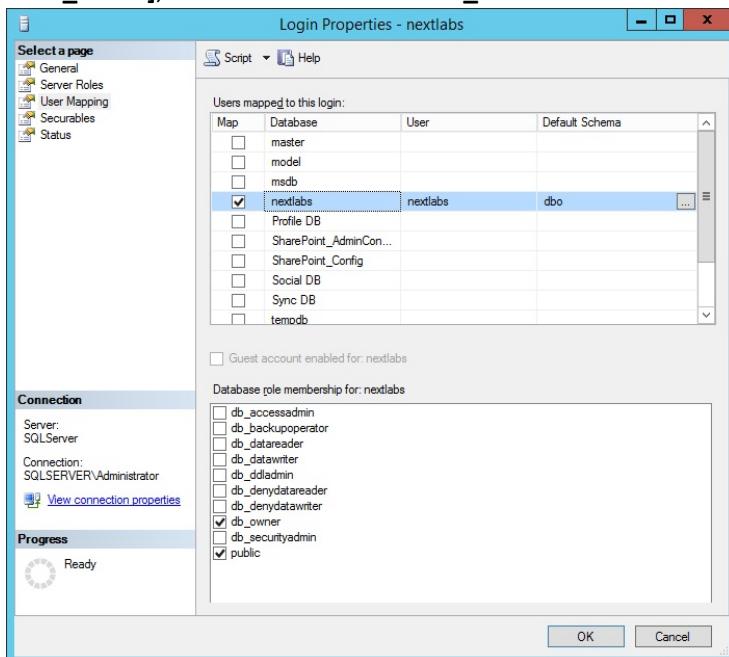
1085

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

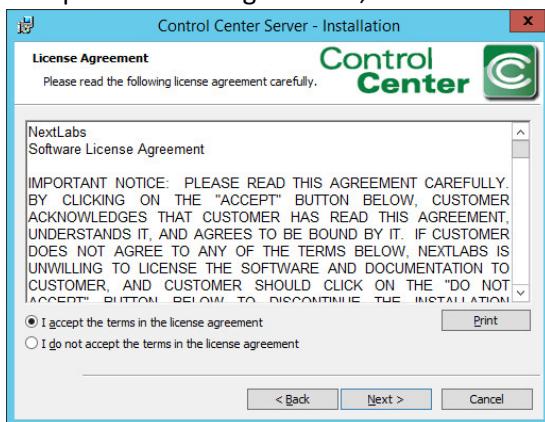


1088

- 1089 9. Click on **User Mapping**, then **New Database**. Under **Database role membership for: [data-**  
 1090 **base\_name]**, check the box next to **db\_owner**.

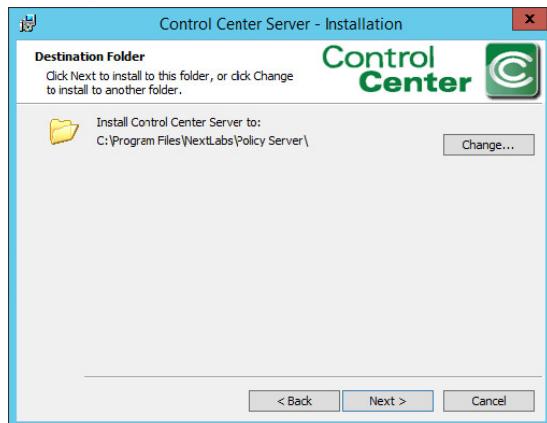


- 1091  
 1092 10. Locate the installation zip file, provided by NextLabs support, and extract it.  
 1093 11. Run the installer as follows:  
 1094   a. On a Windows server, launch Command Prompt as Administrator.  
 1095   b. In the command prompt, navigate to the folder that contains `install.bat`. The  
 1096         following is an example of the `cd` command to type if the installation zip file is extracted  
 1097         in `c:\build`. `cd build\ControlCenter-Windows-chef-- main\PolicyServer`  
 1098 12. From this directory, run the command: `install.bat`  
 1099 13. Click **Next**.  
 1100 14. Accept the license agreement, and click **Next**.



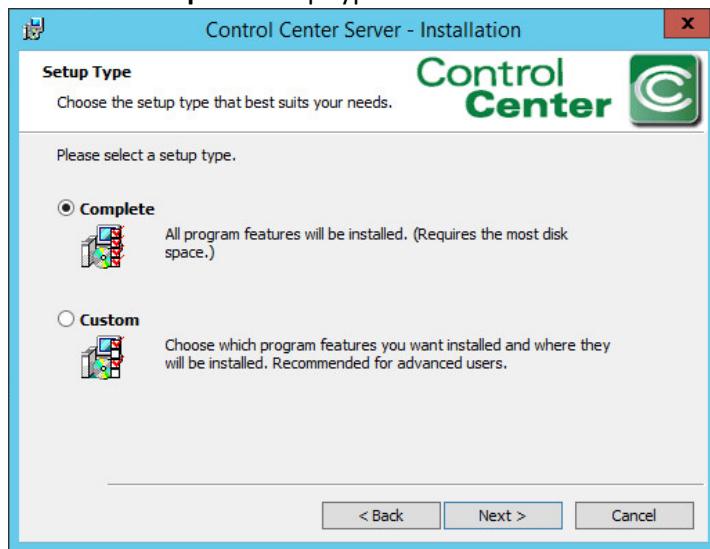
1101

1102 15. Click **Next**.



1103

1104 16. Select the **Complete** setup type. Click **Next**.



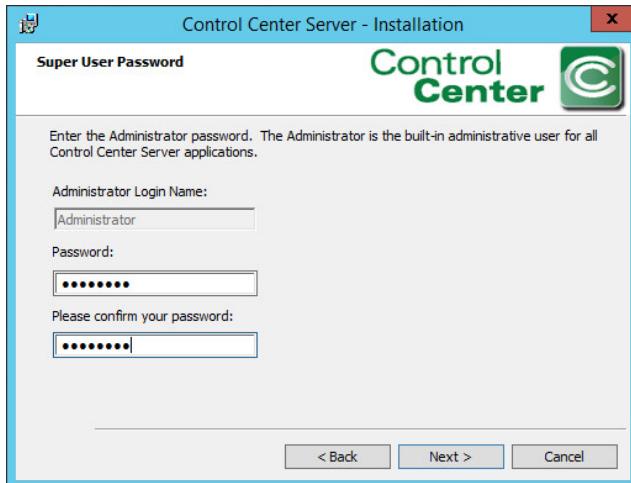
1105

1106 17. Enter the location of the license file. Click **Next**.

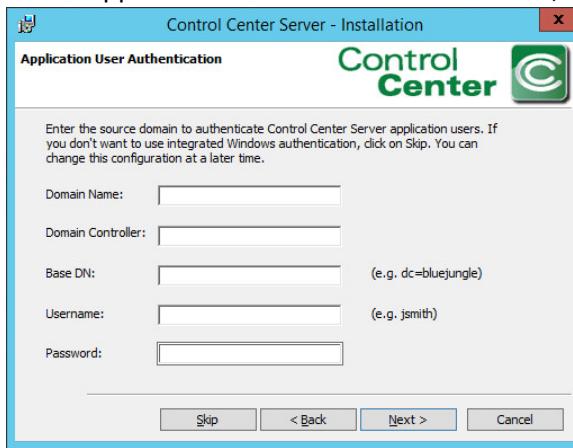


1107

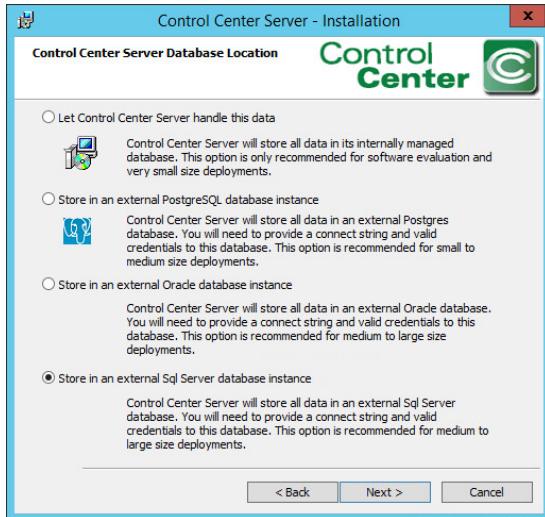
- 1108      18. Enter a Password for the built-in administrative user for all Control Center Server applications.  
 1109      Click **Next**.



- 1110  
 1111      19. Enter a Password to access the SSL certificates for the Control Center Server. Click **Next**.  
 1112      20. Enter a Password to access the Encryption Key Store for the Control Center Server. Click **Next**.  
 1113      21. At the Application User Authentication screen, click **Skip**.

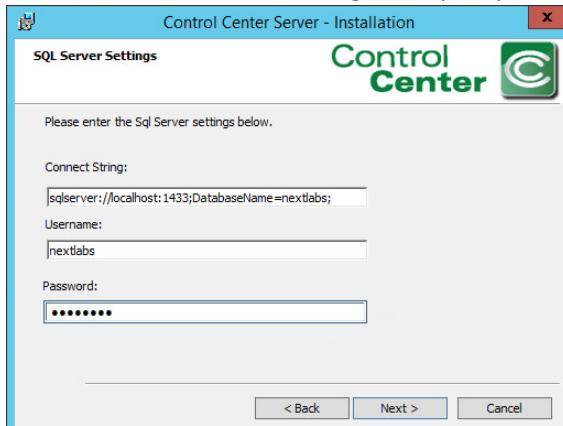


- 1114  
 1115      22. Select **Store in an external Sql Server database instance**. Click **Next**.

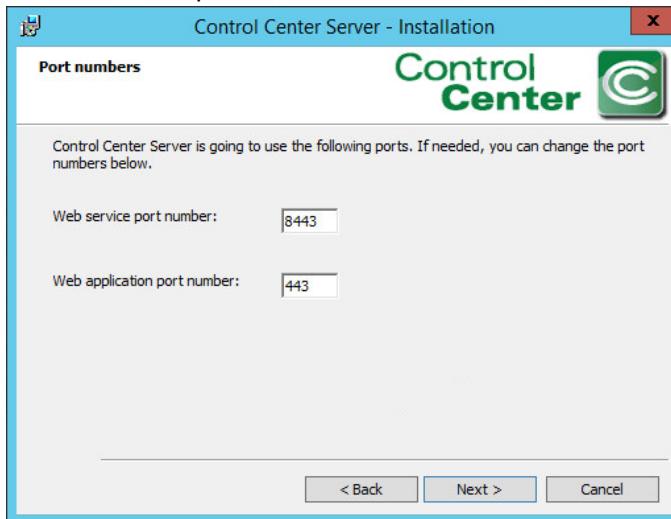


1116

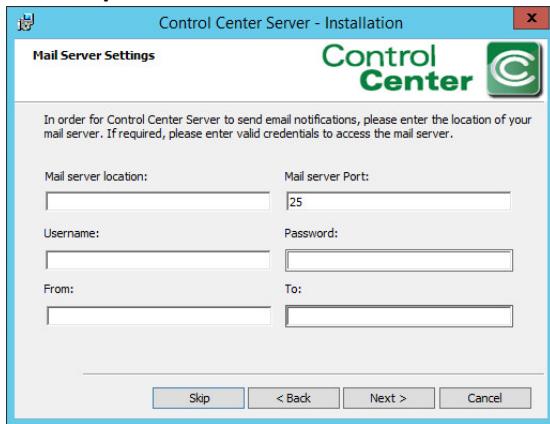
- 1117        23. At the SQL Server settings screen, specify the **Connect String**, **Username**, and **Password**. Make  
 1118        sure the SQL Server is running. It may help to restart the SQL Server.



- 1119  
 1120        24. Use the default port numbers. Click **Next**.



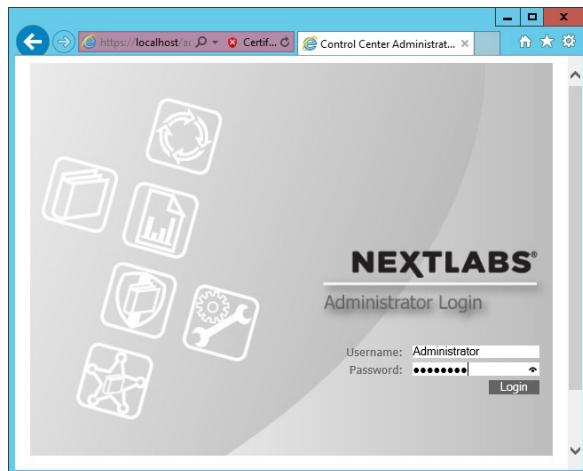
- 1121  
 1122        25. Click **Skip**.



- 1123  
 1124        26. Click **Install**.  
 1125        27. Once completed, click **Finish**.  
 1126        28. Open an Internet browser, navigate to https://localhost/administrator, and log in to the Control  
 1127        Center Administrator web application.

1128

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



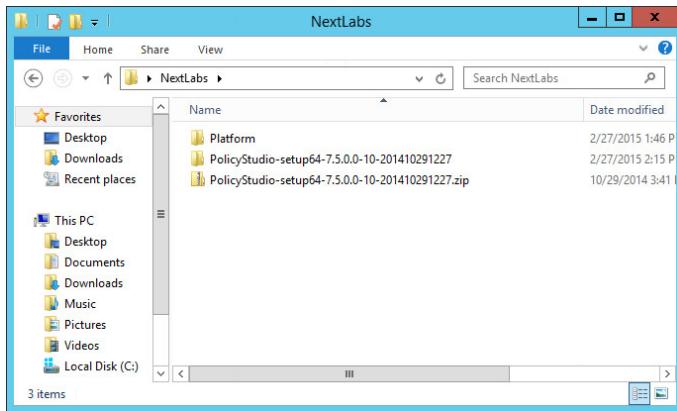
1129

- 1130 29. Once logged in to the Control Center Administrator web application in your browser, you can  
1131 verify that the NextLabs Control Center is installed and configured correctly on the SQL Server.

### 1132 Policy Studio 7.7

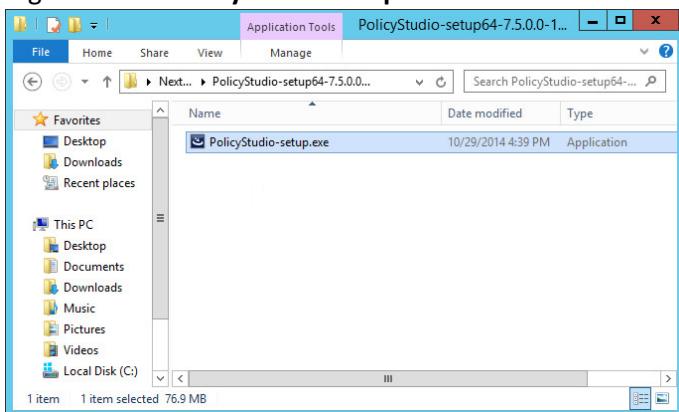
1133 Complete the standard Policy Studio installation per NextLabs documentation available to customers  
1134 using the following steps:

- 1135 1. On the same server, go to your desktop or other known location where the required NextLabs  
1136 Policy Studio installation files are stored.  
1137 2. Right-click on **PolicyStudio-setup64-7.5.0.0-10-201410291227.zip** and select **Extract All**. Wait  
1138 for files to be extracted.

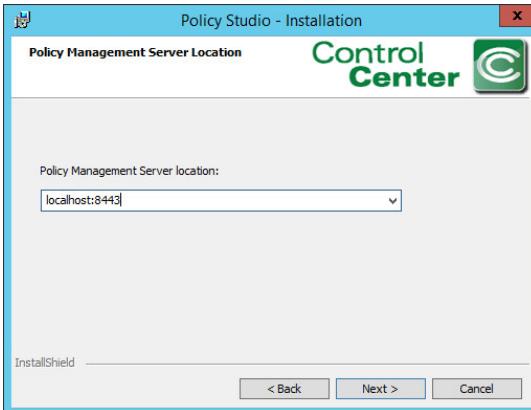


1139

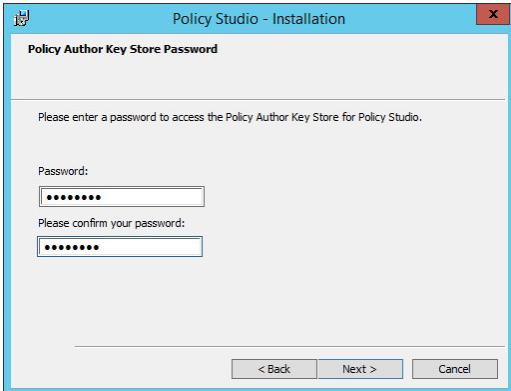
- 1140 3. Double-click to open the **PolicyStudio-setup64-7.5.0.0-10-201410291227** folder.

- 1141 4. Right-click on **PolicyStudio-setup.exe** and select **Run as Administrator**.
- 1142
- 1143 5. At the Welcome to the Installation Wizard for Policy Studio screen of the Policy Studio Installation Window, click **Next**.
- 1144
- 1145
- 1146 6. At the License Agreement screen, select **I accept the terms in the license agreement**, and click **Next**.
- 1147
- 1148
- 
- 
- 

- 1149 7. At the Destination Folder screen, click **Next**.
- 
- 1150 1151 8. At the Policy Management Server Location screen, enter the default location **localhost:8443**.

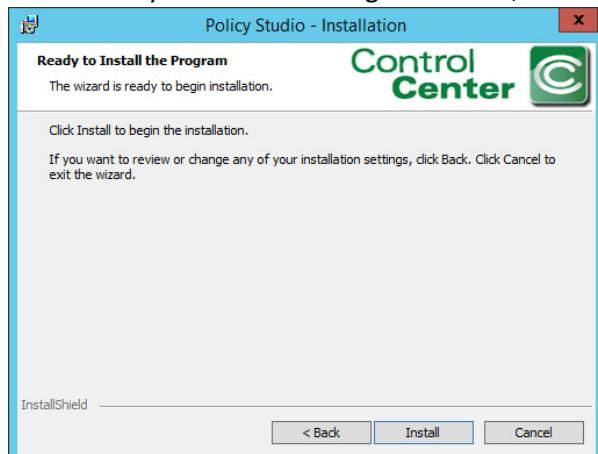


- 1152 1153 Click **Next**.
- 1154 9. At the Policy Author Key Store Password screen, enter a **Password** and click **Next**.

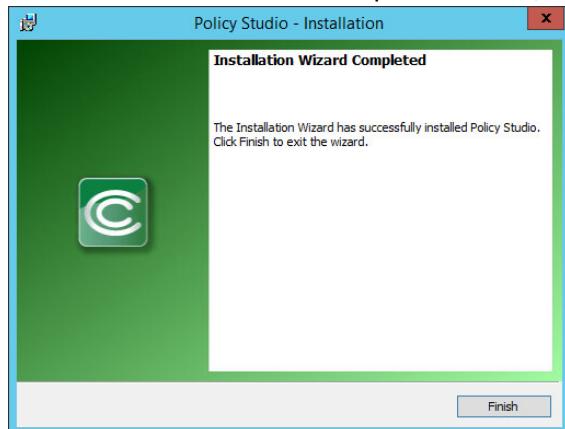


1155

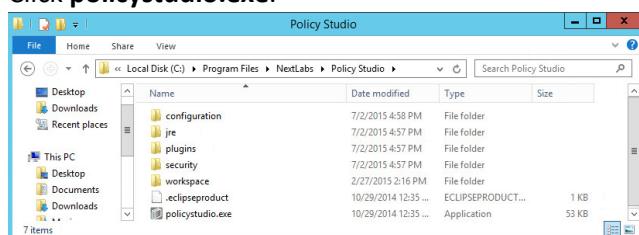
- 1156 10. At the Ready to Install the Program screen, click **Install**.



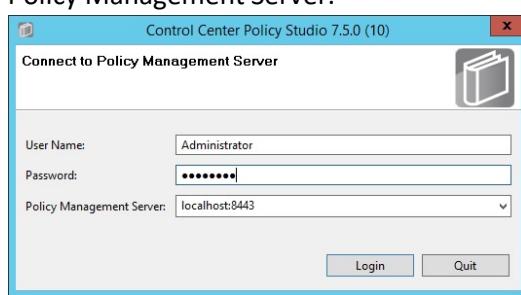
- 1157  
1158 11. At the Installation Wizard Completed screen, click **Finish**.



- 1159  
1160 12. In Windows Explorer, find and open the **policystudio.exe** application file.  
1161 a. Navigate to the **C:/ drive>Program Files>NextLabs>Policy Studio**.  
1162 b. Click **policystudio.exe**.



- 1163  
1164 13. In the Control Center Policy Studio window, enter a **User Name** and **Password** to connect to the  
1165 **Policy Management Server**.



1166

- 1167        14. If the connection is successful, the Control Center Policy Studio - Policy Author window will  
 1168        open. Policies are defined and deployed in this interface.



1169

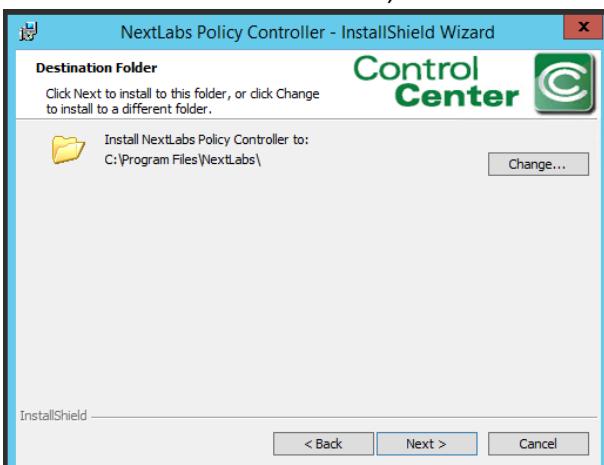
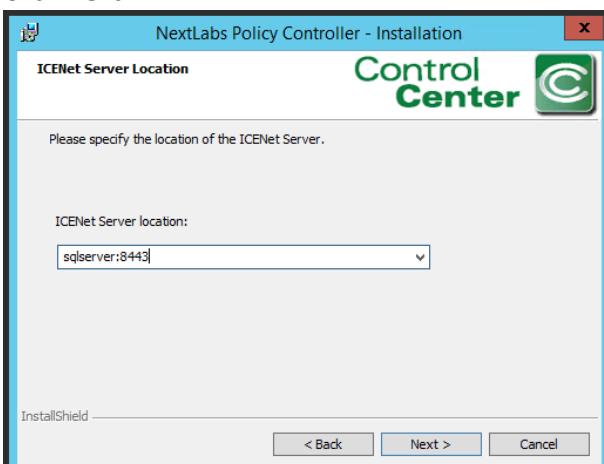
## 1170        Policy Controller 7.7

1171        The Policy Controller is installed on the SharePoint Server. To complete standard Policy Controller  
 1172        installation per NextLabs documentation available to customers, use the following steps:

- 1173        1. On the SharePoint Server, go to your desktop or other known location where the required  
             1174        NextLabs Policy Controller installation files are stored.
- 1175        2. Extract the files from the **PolicyController-CE-64-<version>.zip** file.
- 1176        3. Open the **PolicyController-CE-64-<version>** folder.
- 1177        4. Click **CE-PolicyController-setup64.msi** to begin installation.
- 1178        5. At the Welcome to the InstallShield Wizard for NextLabs Policy Controller Installation screen,  
             1179        click **Next**.
- 1180        6. At the License Agreement screen, select **I accept the terms in the license agreement** and  
             1181        click **Next**.



1182

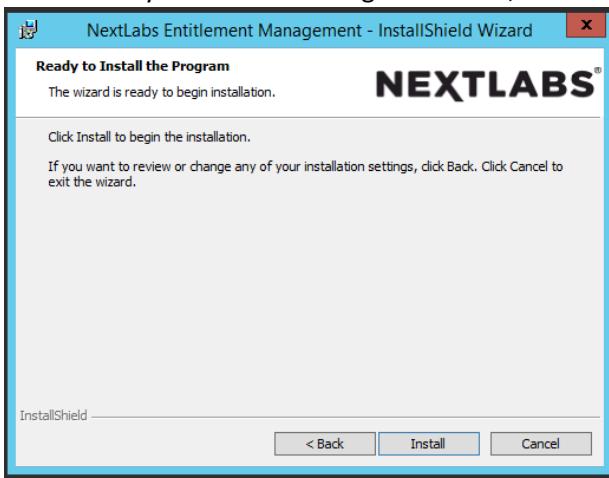
- 1183     7. At the Destination Folder screen, click **Next**.
- 1184
- 
- 1185     8. At the ICENet Server Location screen, enter the default ICENet Server Location: sqlserver:8443. Click **Next**.
- 1186
- 1187
- 
- 1188     9. At the Ready to Install the Program screen, click **Install**.
- 1189
- 
- 1190     10. At the InstallShield Wizard Completed screen, click **Finish**.

1191        11. In the window that immediately opens, click **Yes** to restart the computer, or click **No** to wait and  
 1192            restart after installing Entitlement Manager.

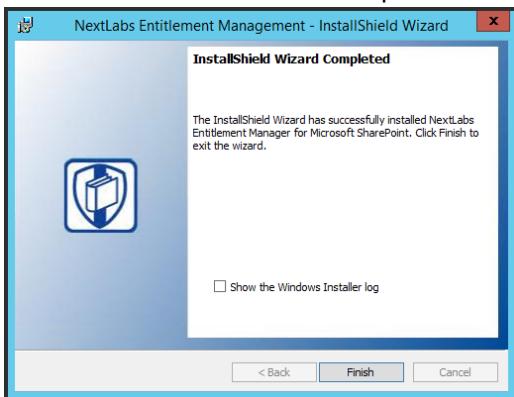
1193        **Entitlement Manager for Microsoft SharePoint 7.6**

1194        Entitlement Manager is installed once SharePoint and the Policy Controller have been installed. The web  
 1195            application site and site collection must already exist in SharePoint. See Section 2.7 for installing  
 1196            SharePoint and creating site collections. Complete the standard Entitlement Manager for SharePoint  
 1197            Server installation per NextLabs documentation available to customers using the following steps.

- 1198        1. On the SharePoint Server, go to your desktop or other known location where the required NextLabs  
             Policy Controller installation files are stored.
- 1200        2. Extract the files from the **SharePointEnforcer-2013-64-<version>.zip** folder.
- 1201        3. Open the **SharePointEnforcer-2013-64-<version>** folder.
- 1202        4. Click on the **SharePointEnforcer-2013-64-<version>.msi** to begin the installation.
- 1203        5. At the Welcome to the InstallShield Wizard for NextLabs Entitlement Manager for MicroSoft Share-  
             Point screen, click **Next**.
- 1205        6. At the License Agreement screen, select **I accept the terms in the license agreement** and click **Next**.
- 1206        7. At the Ready to Install the Program screen, click **Install**.

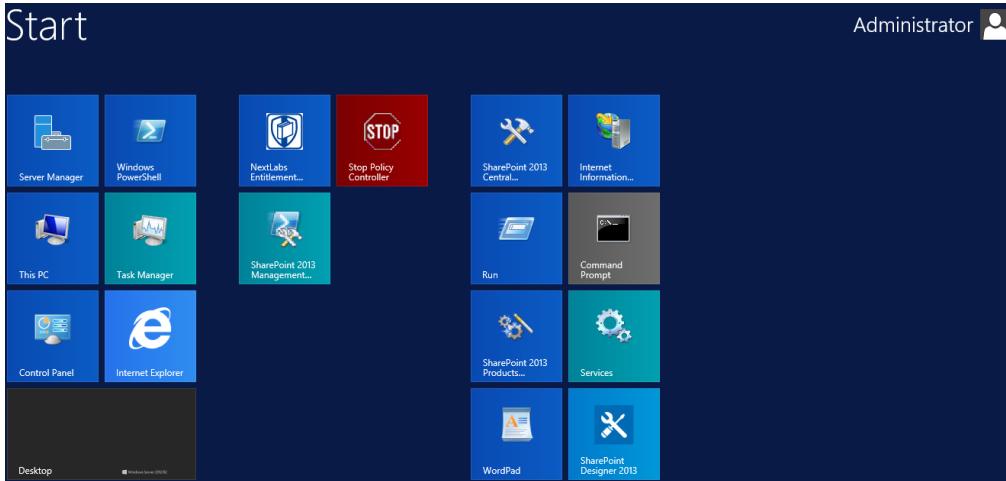


- 1207        1208        8. At the InstallShield Wizard Completed screen, click **Finish**.

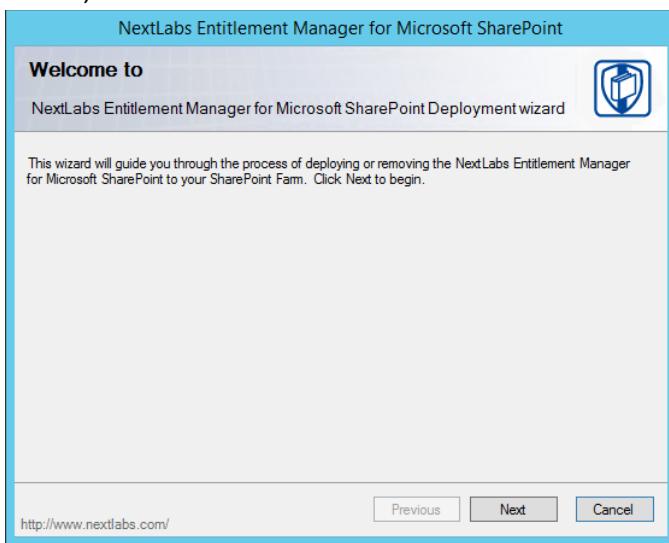


- 1209        1210        9. After installing, the IIS server must be reset:  
 1211            a. Click the Windows icon and begin typing the word **PowerShell** and open the windows  
                   PowerShell application.

- 1213            b. From within the Windows PowerShell window, type in this command and press **Enter** to  
 1214            reset Internet Information Services: **iisreset**.
- 1215        10. On the SharePoint Server, click the **Start** icon to see the applications pinned to the **Start** menu.

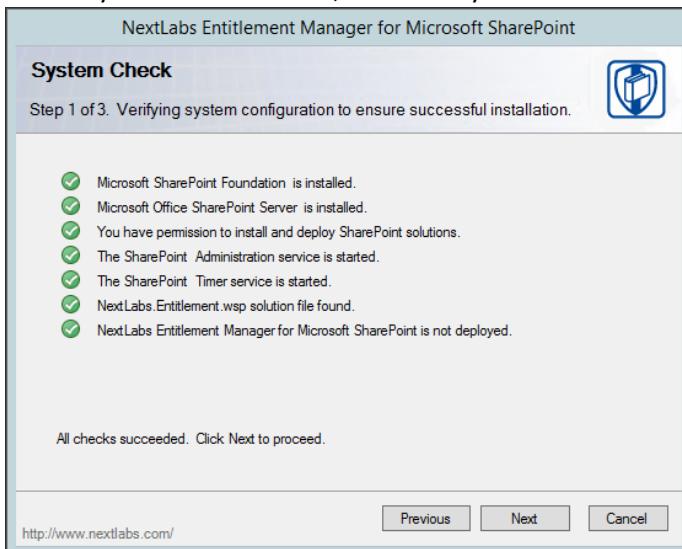


- 1216
- 1217        11. Click the NextLabs Entitlement Manager for SharePoint Server Deployment icon.
- 1218        This shortcut is automatically pinned during the initial installation. In case the shortcut is not created au-  
 1219        tomatically, the application can be opened from File Explorer at the **location: C:\Program**  
 1220        **Files\NextLabs\SharePoint Enforcer\bin\NextLabs.Entitlement.Wizard.exe**
- 1221        12. At the Welcome to NextLabs Entitlement Manager for Microsoft SharePoint Deployment wizard  
 1222        screen, click **Next**.



1223

- 1224 13. At the System Check screen, after the system check is complete, click **Next**.

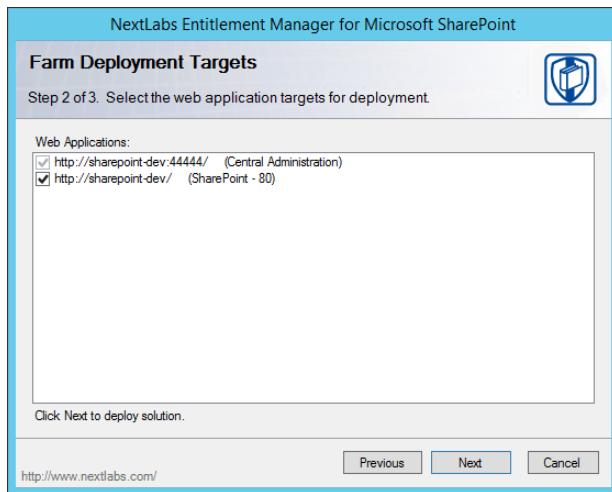


1225

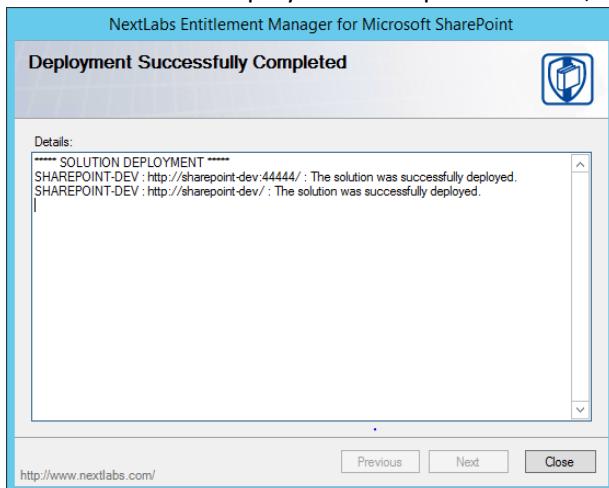
- 1226 14. At the Farm Deployment Targets screen, select the applicable web application on which to deploy.

1227 *Note:* If only one entry is listed, i.e., **http://sharepoint:44444/Central Administration**, no web applications have been created.

- 1229 15. At the Deploying Step 3 of 3 screen, click **Next**.

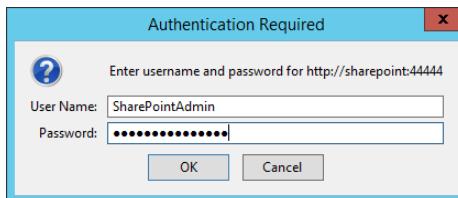


- 1230 16. At the Successful Deployment Completed screen, click **Close**.



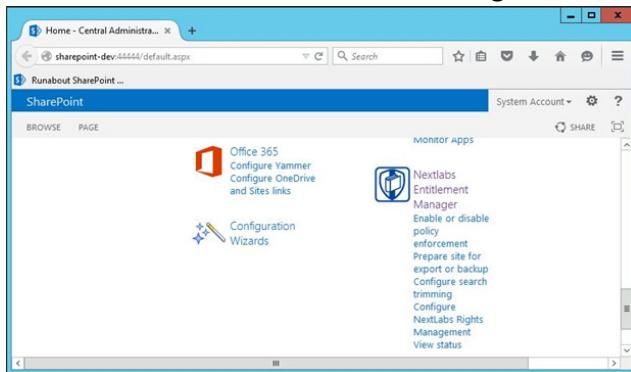
1231

- 1232 17. Open a browser and navigate to the SharePoint Central Administration Portal. Log in with the  
1233 SharePoint Administrator account.



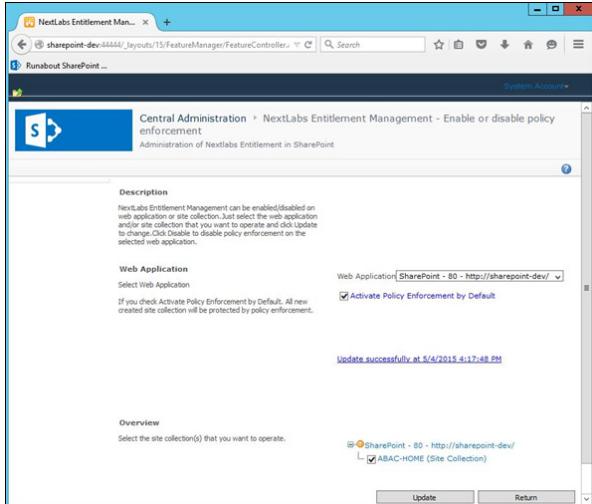
1234

- 1235 18. Click on the **NextLabs Entitlement Manager** icon.



1236

- 1237 19. In the page that opens, scroll down to verify that the correct **Web Application** is chosen and the  
1238 service is **Enabled**.



1239

## 2.5 OpenLDAP

1241 OpenLDAP is an open source implementation of the Lightweight Directory Access Protocol. It stores user  
 1242 identity information along with various other attributes that are indicative of access rights, and it is able  
 1243 to provide the necessary information that requesting services need to make authorization decisions.

### 2.5.1 How It's Used

1244 OpenLDAP stores user information and associated attributes for users who need access to Unix/Linux  
 1245 based applications. Examples of such attributes are a user's userid, group, organizational unit, job title  
 1246 and various other custom attributes. The OpenLDAP service listens and responds to requests from the  
 1247 virtual directory service that acts as the enterprise policy information point and has the responsibility for  
 1248 retrieving, organizing, and aggregating each user's attribute set under a single view.

### 2.5.2 Virtual Machine Configuration

1250 The OpenLDAP virtual machine is configured as follows:

- 1251     ■ Ubuntu Linux 16.04 LTS
- 1252     ■ 1 CPU core
- 1253     ■ 2GB of RAM
- 1254     ■ 2 NICs
- 1255     ■ 60GB of storage
- 1256     ■ OpenLDAP server software

#### 1257 **Network Configuration (Interface 1)**

- 1258     IPv4 Manual
- 1259     IPv6 Disabled
- 1260     IP Address: 192.168.19.11
- 1261     Netmask: 255.255.255.0
- 1262     Gateway: 192.168.19.1

1264 DNS Name Servers 192.168.19.10  
1265 DNS-Search Domains: acmefinancial.com

1266 **Network Configuration (Interface 2)**

1267 IPv4 Manual  
1268 IPv6 Disabled  
1269 IP Address: 192.168.19.11  
1270 Netmask: 255.255.255.0  
1271 Gateway: 192.168.19.1  
1272 DNS Name Servers 192.168.19.10  
1273 DNS-Search Domains: acmefinancial.com

1274 **2.5.3 Firewall Configuration**

1275 Enter the following commands in sequence to allow traffic to LDAPS and SSH ports only.

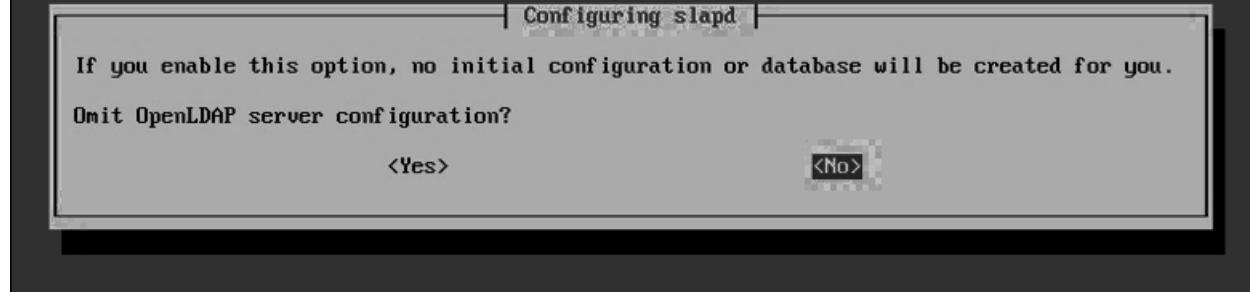
1276 `ufw allow 636/tcp to allow`  
1277 `ufw allow 22/tcp to allow`  
1278 `ufw default deny incoming`

1279 **2.5.4 Installation**

```
root@openldap:~# sudo apt-get install slapd ldap-utils
```

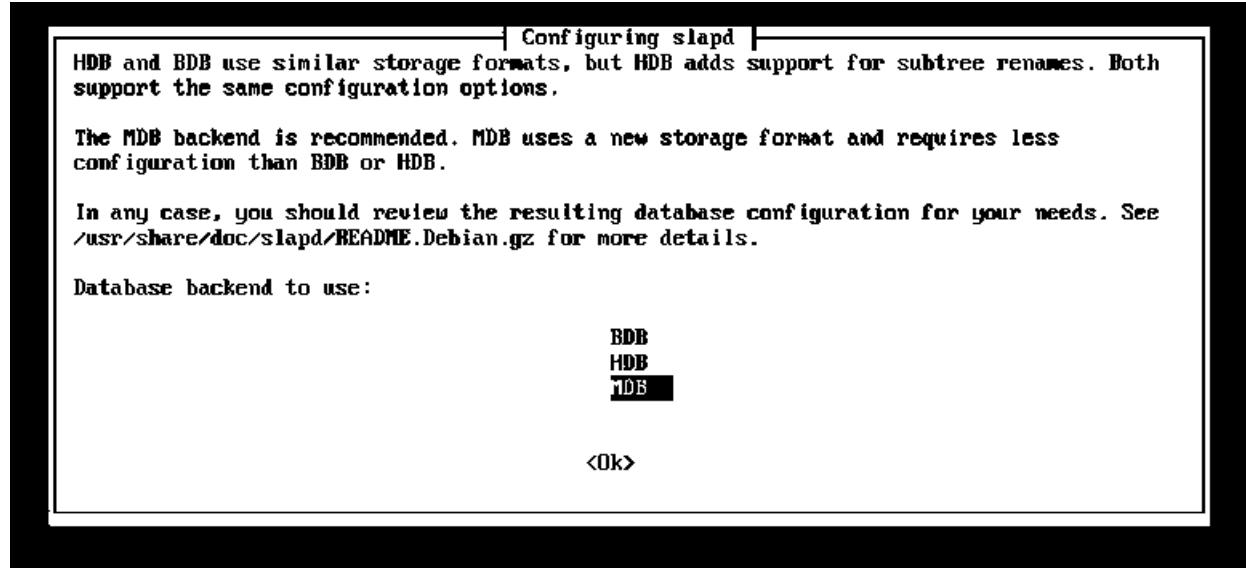
1280

Package configuration



1281

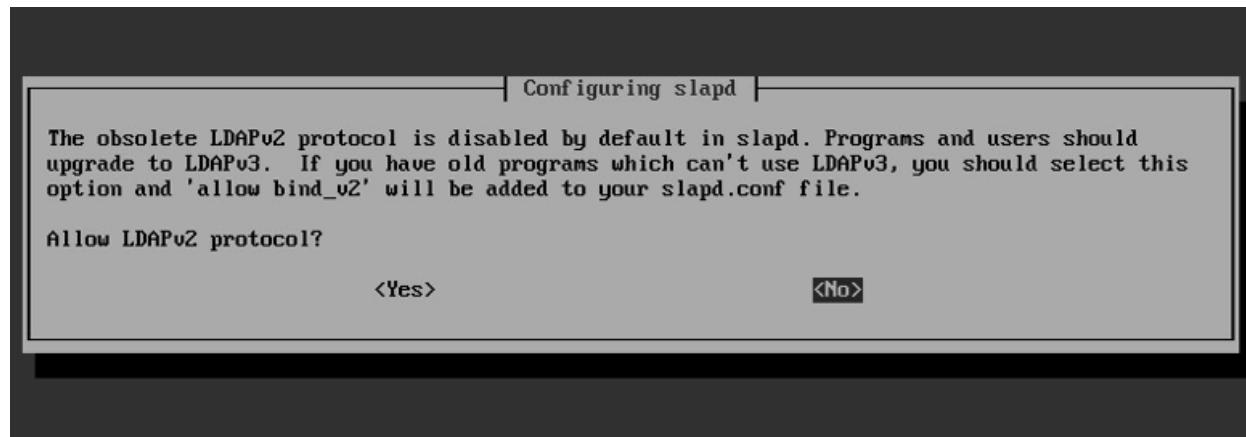
- 1282 1. Select **No** and press **Enter**.
- 1283 2. Enter the organizational Name on the following screen (for example, acmefinancial.com).
- 1284 3. Enter the administrator password for the BaseDN (BaseDN: acmefinancial.com).



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.

- 1294     2. Enter `chown openldap.openldap /etc/ldap/logs` to make the logs subdirectory owned by the  
1295       openldap service.  
1296     3. Enter `touch create-cn-module.ldif` to create a file that will be used to load a cn module. This  
1297       will allow the AuditLogConfig object class to be added. The file contents should be as follows:  
1298            dn: cn=module,cn=config  
1299            objectClass: olcModuleList  
1300            cn: module  
1301            olcModulepath: /usr/lib/ldap  
1302            olcModuleLoad: auditlog.la  
1303     4. Enter `ldapadd -Q -Y -EXTERNAL -H ldap:/// -f create-cn-module.ldif` to add the cn  
1304       module.  
1305     5. Enter `touch logging.ldif`. The file contents should be as follows:  
1306            dn: olcOverlay=auditlog,olcDatabase={1}hdb,cn=config  
1307            changetype: add  
1308            objectClass: olcOverlayConfig  
1309            objectClass: olcAuditLogConfig  
1310            olcOverlay: auditlog  
1311            olcAuditLogFile:/etc/ldap/logs/auditlog.log  
1312     6. Enter `chmod 775 /etc/ldap/logs`.  
1313     7. Enter `chmod 664 /etc/ldap/logs/auditlog.log`.  
1314     8. Enter `ldapadd -Q -Y -EXTERNAL -H ldap:/// -f logging.ldif`.  
1315     9. Changes to user records should now appear in `/etc/ldap/logs/auditlog.log`.

### 2.5.6 STARTTLS and LDAPS Configuration

- 1316     1. On the OpenLDAP server, create an ssl directory `/etc/ldap/ssl`. Enter `mkdir /etc/ldap/ssl`.  
1317     2. Move the certificates created for the OpenLDAP server from the Certificate of Authority to the  
1318       ssl subdirectory:  
1319            a. `scp openldap_cert.pem user1@openldap.acmefinancial.com:\ldap\ssl`  
1320            b. `scp openldap_privatekey.pem user1@openldap.acmefinancial.com:\ldap\ssl`  
1321            c. `scp acmefinancial.com-CA.pem user1@openldap.acmefinancial.com:\ldap\ssl`  
1322     3. Install the CA certificate so that local applications can use the certificate when necessary:  
1323            a. `cp acmefinancial.com-CA.pem /usr/share/ca-certificates/acmefinancial.com-CA.crt`  
1324            b. Add `acmefinancial.com-CA.crt` to the end of the `/etc/ca-certificates.conf` file.  
1325            c. Enter `sudo update-ca-certificates`.  
1326     4. Create a certificate information file called `certinfo.ldif` in `/etc/ldap/ssl` with the following con-  
1327       tents:

```

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

```

- 1322 5. Set permissions and ownership on the certificate files so that the openLDAP user can read the  
 1323 key file:

- `sudo adduser openldap ssl-cert`
- `chgrp ssl-cert /etc/ldap/ssl/openldap_privatekey.pem`
- `chmod g+r /etc/ldap/ssl/openldap_privatekey.pem`
- `chmod o-r /etc/ssl/ldap/openldap_privatekey.pem`
- `chown root.ssl-cert /etc/ldap/ssl/openldap_privatekey.pem`
- `chown root.ssl-cert /etc/ldap/ssl/openldap_cert.pem`
- `chmod root.ssl-cert /etc/ldap/ssl`

- 1332 6. Reconfigure slapd by running the following command
- `ldapmodify -Y EXTERNAL -H ldap:/// -f /etc/ldap/ssl/certinfo.ldif`
  - Restart slapd by running **service slapd restart**

1335 StartTLS should now be enabled.

- 1336 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 also
# 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:///"

```

- 1339 a. Go to the `SLAPD_SERVICES` line and add `ldaps://` as shown above.  
 1340 b. Enter **service slapd restart** to restart the OpenLDAP service.

- 1341 8. Prepare the slapd client to use StartTLS:  
 1342 a. Create the `/etc/ldap/ssl` directory.  
 1343 b. Copy `acmefinancial.com-CA.pem` to `/etc/ldap/ssl/` directory.  
 1344 c. Go to the client computer and edit `/etc/ldap/ldap.conf`.  
 1345 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

```

1348 **2.5.7 Formatting Audit Logs**

1349 The file */etc/ldap/logs/auditlog.log* stores log entries destined for the Splunk indexer. Using the follow-  
 1350 ing scripts, the logs were formatted in such a way that enables the Splunk indexer to easily determine  
 1351 the start and end of each log event.

1352 **2.5.8 Script: /etc/ldap/logs/auditlogscript**

```
1353 #!/bin/bash
1354 # Remove newlines, make file a single string and dump to auditlog.string
1355 tr -s '\n' '' < /etc/ldap/logs/auditlog.log > /etc/ldap/logs/auditlog.string
1356 # Change every occurrence of #0 to just 0
1357 sed -i -e 's/#0/0/g' /etc/ldap/logs/auditlog.string
1358 # Remove spaces between attributes and their values
1359 sed -i -e 's/: /:/g' /etc/ldap/logs/auditlog.string
1360 #Additional formatting helpful in showing field separation
1361 sed -i -e 's/ /;;/g' /etc/ldap/logs/auditlog.string
1362 # Change # to newline making each line a unique openldap event and dump
1363 # to auditlog.lines
1364 tr -s '#' '\n' </etc/ldap/logs/auditlog.string> /etc/ldap/logs/auditlog.lines
1365 #Additional formatting in removing unneeded lines
1366 sed -i ';;end;;/d' /etc/ldap/logs/auditlog.lines
1367 # Empty previous contents of outlog.log
1368 # outlog.log is effectively overwritten when script runs
1369 cp /dev/null /etc/ldap/logs/outlog.log
1370 # Call add-timestamp.py to add readable timestamps and dump to outlog.log
1371 /etc/ldap/logs/add-timestamp.py
```

1372 **2.5.9 Script: /etc/ldap/logs/add-timestamp.py**

```
1373#!/usr/bin/python3
1374import datetime
1375start_index = 0
1376end_index = 0
1377timestamp = 123456789 #var to store datetime object; values are placeholders
1378localtime = "12345" #string var to store local time; values are placeholders
1379filename = "/etc/ldap/logs/auditlog.lines" #Each event in file is a line
1380#Open the file, parse each each line,identified char set in IF
1381#statement exposing the epoch_time without leading or trailing chars
1382with open(filename, 'r') as file_object:
1383    for string in file_object:
1384        if ";;dc" in string:
1385            end_index = string.find(";;dc")
1386            string = string.strip()
1387            newstring = string[start_index:end_index]
1388            newstring = newstring.lstrip(';;')
1389            newstring = newstring.lstrip('add')
1390            newstring = newstring.lstrip('modify')
1391            newstring = newstring.lstrip('delete')
1392            newstring = newstring.lstrip('rdn')
1393            newstring = newstring.lstrip(';;')
1394            epoch_time = int(newstring) #Store epoch_time as integer
1395            #Convert epoch_time to datetime object and store in timestamp
1396            timestamp = datetime.datetime.fromtimestamp(epoch_time)
1397            #Convert value in timestamp to string and store in localtime
1398            localtime = str(timestamp)
1399            #If line is blank, do nothing, else prepend localtime to line
1400            if string.isspace():
1401                pass
1402            else:
```

```

1403         with open('/etc/ldap/logs/outlog.log', 'a') as outfile_object:
1404             outfile_object.write(localtime + string + '\n')
1405 2.5.10 Script: /etc/cron.daily/openldap-status
1406 #!/bin/bash
1407 #This script sends online status updates to splunk with enough information
1408 #such that analytics on Splunk can determine whether or not this host has
1409 #failed to send updates in a given period.
1410
1411 if ls /var/log/oldstatustime # check if file exists
1412 then
1413     prevtime=$(cat /var/log/oldstatustime) #store date in file in variable prevtime
1414 else
1415     date >/var/log/oldstatustime #else write current date to file path
1416 fi
1417 #write time hostname previous run time and online keyword to file path
1418 #in a single line separated by commas
1419 ((date && hostname && echo $prevtime && echo online)|tr -s '\n' ','|sed
1420 s'/online,/online/';echo "") >> /var/log/openldap-status-file.csv
1421 date > /var/log/oldstatustime

```

## 1422 **2.6 Radiant Logic**

1423 Radiant Logic RadiantOne Virtual Directory Server (VDS) is a virtual directory that performs a federated  
1424 identity service. (Note: Radiant Logic changed their product name from RadiantOne Virtual Directory  
1425 Server (VDS) to RadiantOne Federated Identity Service (FID)).

### 1426 **2.6.1 How Its Used**

1427 The RadiantOne VDS (VD) is used in two capacities in this example implementation. First, the VD acts as  
1428 a federated identity service, correlating users from each directory into a single view. Second, the VD acts  
1429 as a monitoring service, where the created view is cached, and changes made to the cache are logged  
1430 and sent to Splunk.

### 1431 **2.6.2 Virtual Machine Configuration**

1432 The Radiant Logic virtual machine is configured as follows:

- 1433     ▪ Ubuntu Linux 16.04 LTS
- 1434     ▪ 4 CPU cores
- 1435     ▪ 24GB of RAM
- 1436     ▪ 2 NICs
- 1437     ▪ 100GB of storage

#### 1438 **Network Configuration (Interface 1)**

1439 IPv4 Manual  
1440 IPv6 Disabled  
1441 IP Address: 192.168.17.100  
1442 Netmask: 255.255.255.0  
1443 Gateway: 192.168.17.1

1444 DNS Name Servers: 192.168.17.1  
 1445 DNS-Search Domains: n/a

#### 1446 **Network Configuration (Interface 2)**

1447 IPv4 Manual  
 1448 IPv6 Disabled  
 1449 IP Address: 192.168.14.111  
 1450 Netmask: 255.255.255.0  
 1451 Gateway: 192.168.14.1  
 1452 DNS Name Servers 192.168.14.1  
 1453 DNS-Search Domains: n/a

#### 1454 **2.6.3 Installing the Virtual Directory**

1455 To install the VD, see the documentation provided with the software. The VD installation guide can also  
 1456 be found on the Radiant Logic support website [here](#).

#### 1457 **2.6.4 Configuring VD**

1458 Steps for configuring the VD are as follows:

- 1459     ■ Add server backends.
- 1460     ■ Create proxy backend.
- 1461     ■ Configure caching and system connectors.
- 1462     ■ Create SharePoint view.
- 1463     ■ Log Settings.

1464 To add the server backends in the VD, complete the following steps:

- 1465     1. While logged in as the Directory Manager, navigate to **Settings>Server Backend>LDAP Data Sources**,
- 1466     2. Click **Add**.

Name	Type	Host	Port
fs arm aggre	LDAP	localhost	2389
fsarm ad	LDAP	192.168.19.10	389
openldap	LDAP	192.168.19.11	389
racf	LDAP	172.17.212.10	389
replicationjournal	LDAP	RadiantOneVDS	2389
vdsha	LDAP	RadiantOneVDS	2389

1468

- 1469     3. Name the data source and enter the parameters. For AD, the parameters used are shown in the  
 1470     following screenshot. Click **Save**.

Server Backend » LDAP Data Sources » Edit LDAP Data Source

**Edit LDAP Data Source**

Data Source Name: fsarm ad

Data Source Type: AD2008 Status: Active

Host Name: 192.168.19.10

Bind DN: Administrator@acmefinancial.com

Base DN: DC=AcmeFinancial,DC=com

Port: 389 SSL

Bind Password:

Use Kerberos profile: vds\_krb5

Disable Referral Chasing

Paged Results Control, page size: 600

Verify SSL Certificate Hostname

**Test Connection**

**Failover LDAP Servers**

**Advanced**

- 1471     Note: Be sure to select **Disable Referral Chasing** for AD.  
 1472  
 1473     4. Repeat Steps 2 and 3 for the OpenLDAP and RACF directories. Use LDAP as the data source type.  
 1474     Details for each are shown in the following screenshots:

Server Backend » LDAP Data Sources » Edit LDAP Data Source

**Edit LDAP Data Source**

Data Source Name: openldap

Data Source Type: LDAP Status: Active

Host Name: 192.168.19.11

Bind DN: cn=admin,dc=acmefinancial,dc=com

Base DN: dc=acmefinancial,dc=com

Port: 389 SSL

Bind Password:

Use Kerberos profile: vds\_krb5

Disable Referral Chasing

Paged Results Control, page size: 0

Verify SSL Certificate Hostname

**Test Connection**

**Failover LDAP Servers**

**Advanced**

Server Backend » LDAP Data Sources » Edit LDAP Data Source

**Edit LDAP Data Source**

Data Source Name: racf

Data Source Type: LDAP Status: Active

Host Name: 172.17.212.10

Bind DN: racfid=TSNI00,profiletype=user,SYSPLEX=SYSPLEX1

Base DN: SYSPLEX=SYSPLEX1

Port: 389 SSL

Bind Password:

Use Kerberos profile: vds\_krb5

Disable Referral Chasing

Paged Results Control, page size: 0

Verify SSL Certificate Hostname

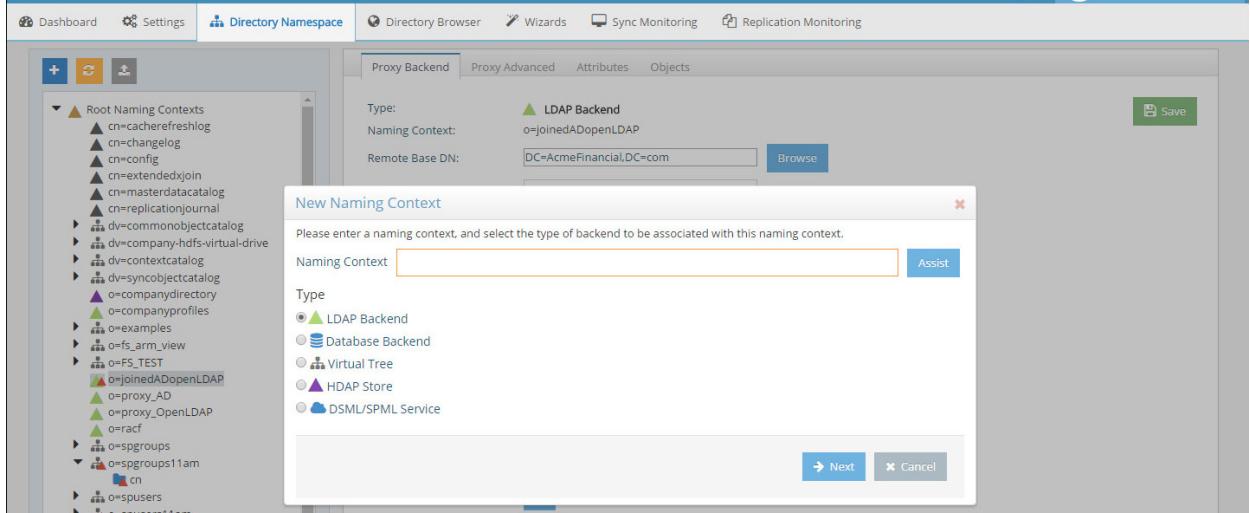
**Test Connection**

**Failover LDAP Servers**

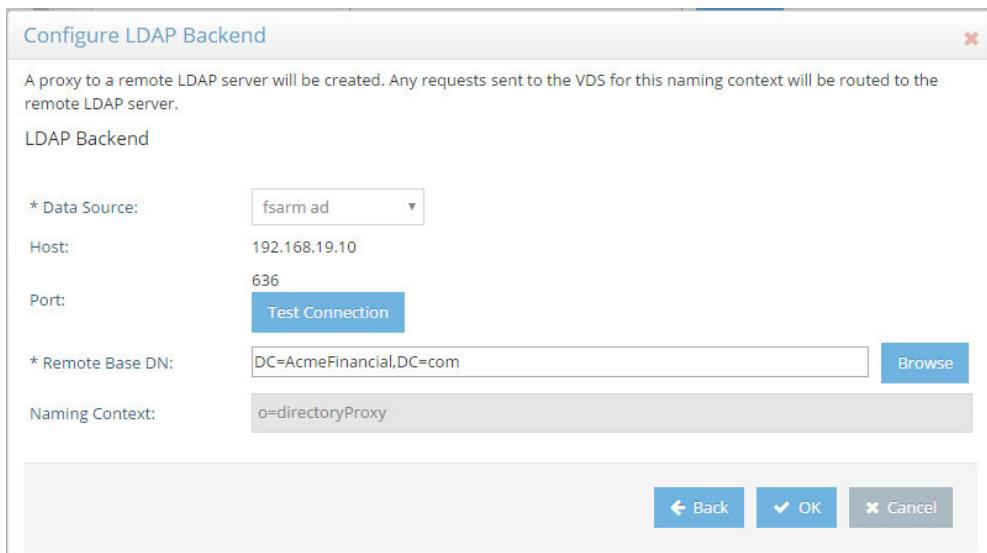
**Advanced**

- 1475  
 1476     1477     To create a proxy view to the backend directories, complete the following steps:

- 1478     1. On the Directory Namespace tab, select **New Naming Context** (the plus sign) at the top left of  
 1479       the screen.  
 1480     2. Select the **LDAP Backend** radio button and enter a naming context such as o=directoryProxy.  
 1481       Select **Next**.

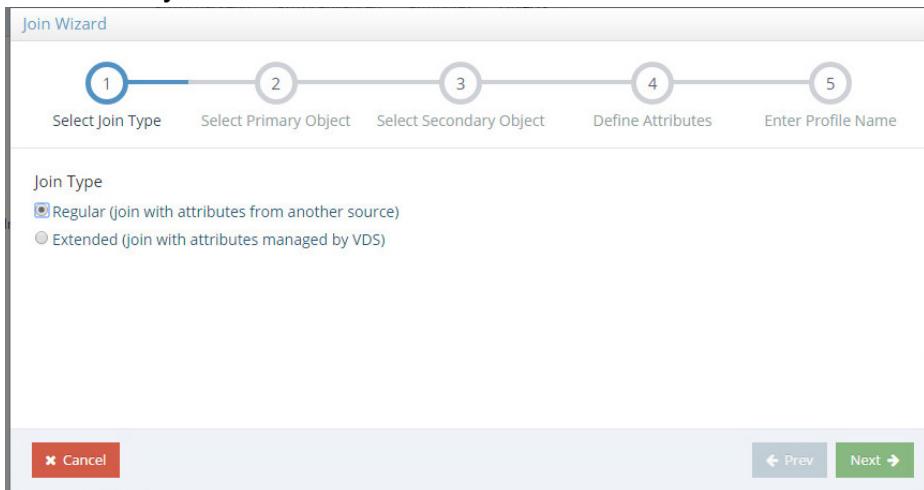


- 1482     3. Select the name of the AD backend created earlier as the **Data Source**. Select the **Remote Base**  
 1483       **DN** of the domain. Select **OK**.



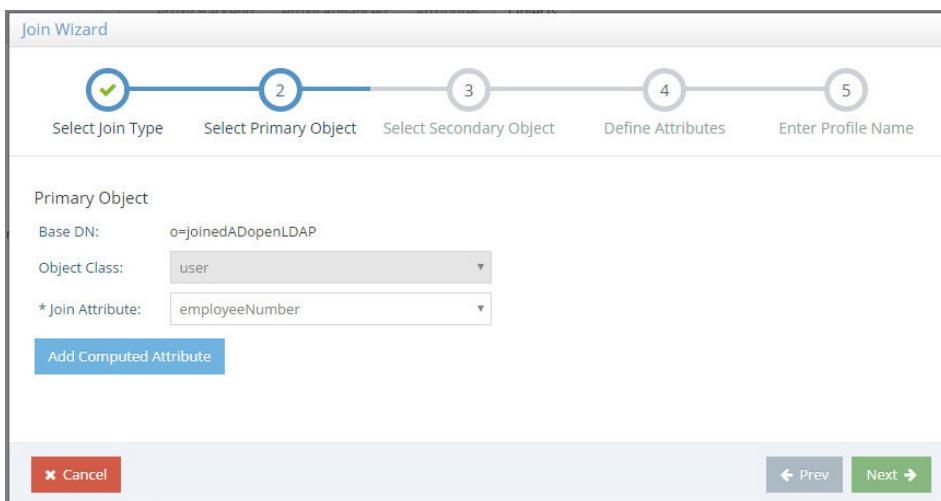
- 1485     4. When the LDAP proxy is created, select the root naming context created in the left window  
 1486       pane.

- 1488 5. Select the **Objects** Tab. Select **New** under **Join Profiles**.



1489  
1490  
1491  
1492

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



1493 employeeNumber attribute should be the same in both sources for that employee.  
1494 8. Select **openLDAP** as the **Data Source** and enter **dc=acmefinancial,dc=com** as the **Base DN**.  
1495 Specify **sub** as the **Scope**, **inetOrgPerson** as the **Object Class**, and **employeeNumber** as the **Join**  
1496 **Attribute**. Leave **Size Limit** as default. Click **Next**.

Join Wizard

Select Join Type    Select Primary Object    **Select Secondary Object**    Define Attributes    Enter Profile Name

**Secondary Object**

Data Source: openldap  
192.168.19.11:636

\* Base DN: dc=acmefinancial,dc=com [Browse](#)

Scope: sub

Size Limit: 0

\* Object Class: InetOrgPerson

\* Join Attribute: employeeNumber

**Condition**

\* Join Condition: (&(employeeNumber=@[employeeNumber:varchar])(objectclass/inetOrgPerson))

[Cancel](#) [Next →](#)

1497

1498

## 9. Select All Attributes. Click Next.

Join Wizard

Select Join Type    Select Primary Object    Select Secondary Object    **Define Attributes**    Enter Profile Name

Return attributes

All attributes

Attributes listed below:

[+ Add](#) [Remove](#)

Actual Name	Virtual Name
audio	
businessCategory	
carLicense	
cn	
departmentNumber	

[Cancel](#) [Next →](#)

1499

1500

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

Join Wizard

Select Join Type    Select Primary Object    Select Secondary Object    Define Attributes    Enter Profile Name

Profile Name

\* Join Profile Name:

1501

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

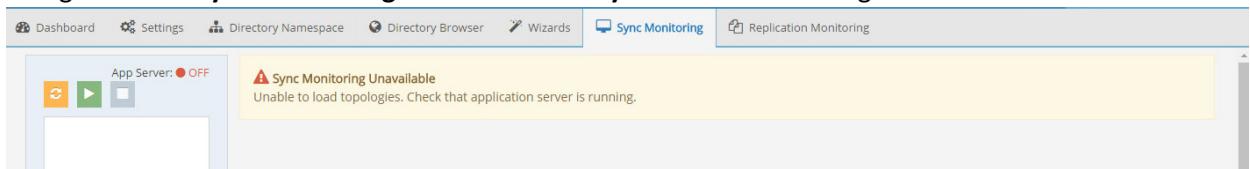
1504

## 2.6.5 Configure Logging

1505 To log changes to each directory object, you must create a cache for the proxy view created in the  
1506 previous section. To create the cache and log changes made to the backend directories, complete the  
1507 following steps:

1508

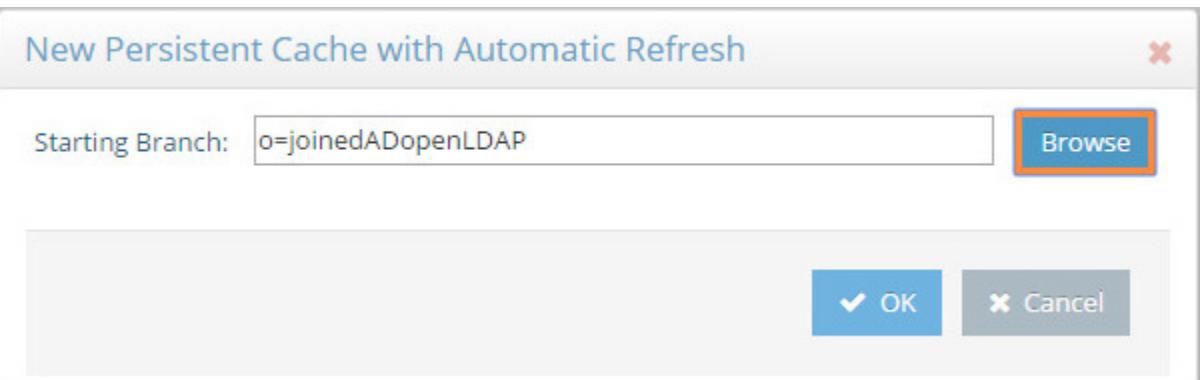
1. Navigate to the **Sync Monitoring** tab. Press the **Play** button to start the glassfish server.



1509

- 1510      2. In the **Directory Namespace** tab, highlight **Cache** in the left window pane. Select **Persistent Cache with Automated Refresh**. Click **Create Persistent Cache**.

- 1512      3. Browse and select the LDAP proxy created in the previous section. Select **OK**. The VD creates the  
1513      cache.  
1514

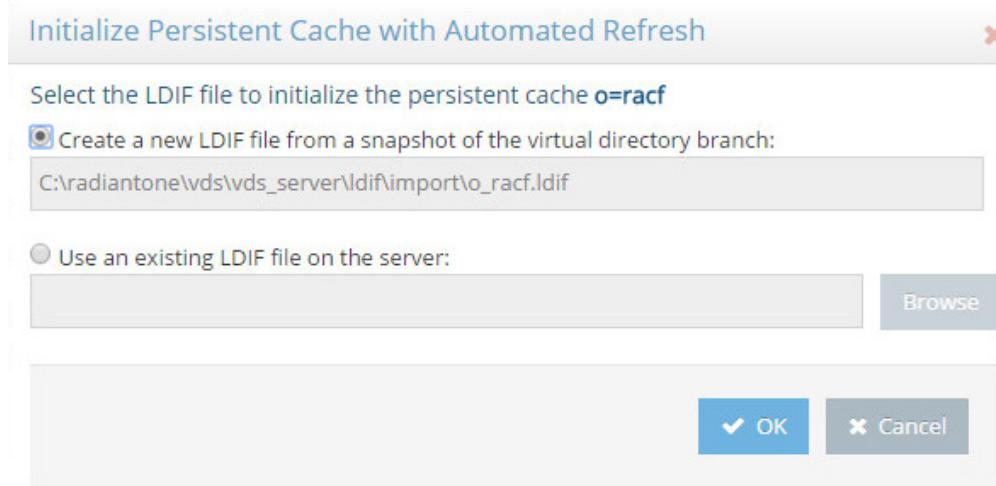


1515

- 1516 4. Select the created cache from the lower left window. Click **Initialize** to make the cache active.

The screenshot shows the 'Properties' tab of the 'Directory Namespace' configuration interface. On the left, a tree view lists 'Root Naming Contexts' and a 'Cache' section containing three entries: 'o=joinedADOpenLDAP', 'o=spgroups11am', and 'o=spusers11am'. The right panel displays the 'Persistent Cache with Automated Refresh' settings. Key fields include 'Starting Suffix': 'o=joinedADOpenLDAP', 'Internal Suffix': 'o=joinedADOpenLDAP', and 'Storage Name': 'Cache'. Other settings like 'Non-indexed Attributes', 'Sorted Attributes', and 'Encrypted Attributes' are also visible. A 'Configure' button is at the bottom left, and a 'Save' button is at the top right. A watermark for 'Activate Windows' is present in the background.

- 1517  
1518 5. Select **Create a new LDIF file from a snapshot of the virtual directory branch**. Click **OK**. This step  
1519 may take a while depending on the number of accounts in the backend directories.



- 1520  
1521 6. Once complete, **Save** the settings.  
1522 7. Select the **Connectors** tab.

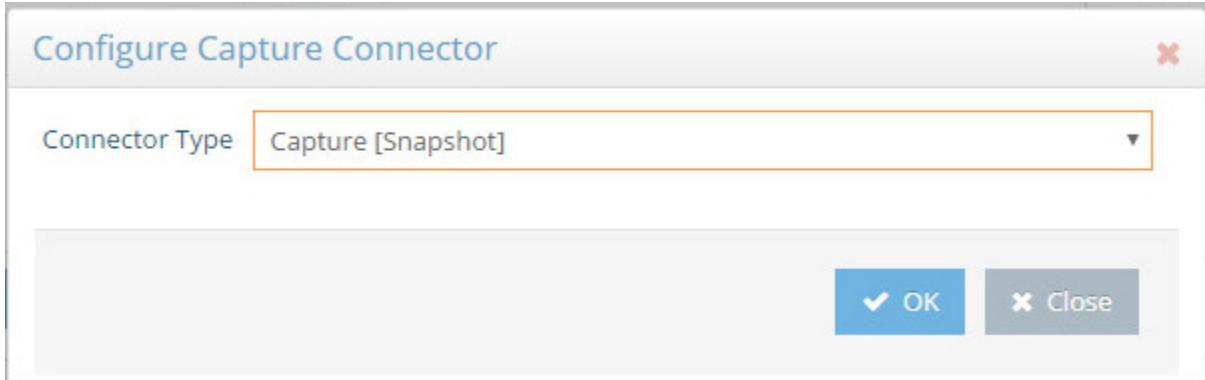
The screenshot shows the 'Connectors' tab of the 'Properties' interface. Under 'Cache Refresh Connectors', the topology is set to 'CF\_O\_JOINEDADOPENLDAP'. It features a table of connectors:

Connector	Type	Status
ds_opendap__dc_acmefinancial_dc_com-inetOrgPerson	Capture [Snapshot]	STOPPED
o_joinedadopenldap-generic	Capture [Snapshot]	STOPPED
vdsconnector-cacherefresh	Apply [LDAP]	STOPPED

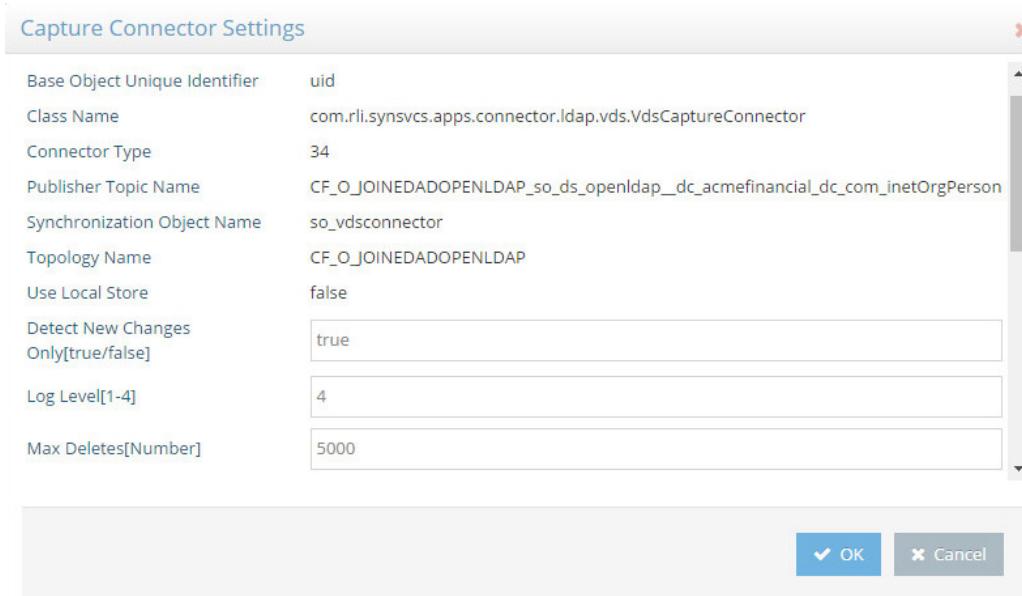
At the bottom are buttons for 'Configure', 'Settings', 'Start', 'Stop', 'Suspend', 'Log', and 'Error Details'.

- 1523

- 1524        8. There should be a connector for each backend directory and one for the connector itself.  
 1525        Highlight the first connector. Select **Configure**. Change the connector type to "Capture  
 1526        [Snapshot]." Click **OK**. Repeat this step for each connector except the "vdsconnector-  
 1527        cacherefresh."

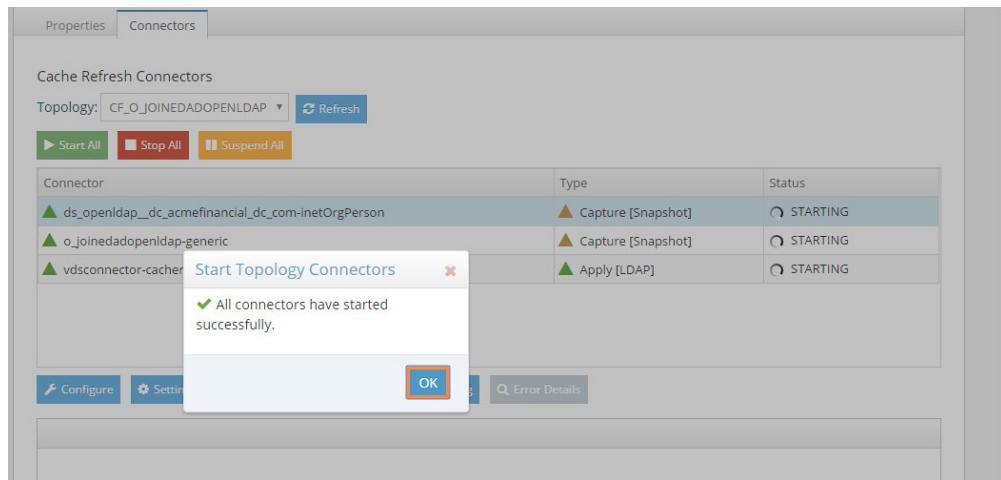


- 1528        9. Back at the **Connectors** tab, highlight the first connector. Select **Settings**. Change the log level to  
 1529        the number 4. Click **OK**. Repeat this step for each connector except the "vdsconnector-  
 1530        cacherefresh."



1532

- 1533 10. Select **Start All** to start all the connectors. Click **OK**.



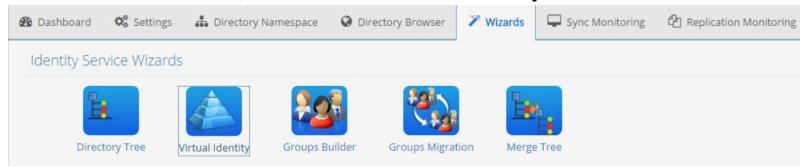
- 1534  
1535 11. If the **Status** from each connector reads STARTED, you are done with this step. If not, review the  
1536 logs and check the connections to the backend databases.



- 1537  
1538 2.6.6 Configure Views for SharePoint  
1539 For applications to perform a global search (identify a user and locate groups) in the virtual namespace  
1540 and be able to locate entries from many different types of underlying sources, the schemas must be  
1541 mapped to a common naming context. There are many possible ways to configure virtual views for  
1542 identities. We will leverage the Virtual Identity Wizard and the Groups Builder Wizard. For more details  
1543 on each wizard, refer to the *RadiantOne System Admin Guide*. This guide is available on request.

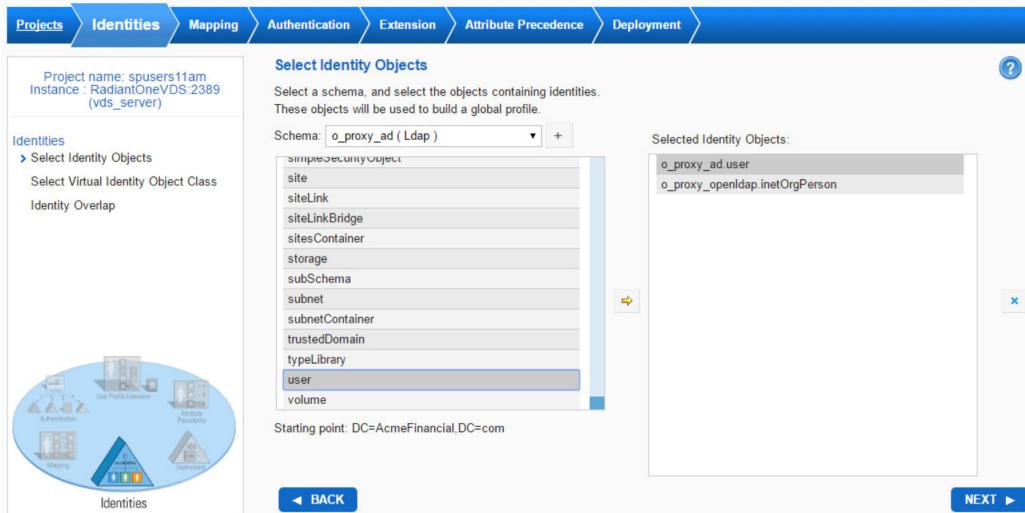
1544 To configure the Virtual Identities for SharePoint, follow these steps:

- 1545 1. On the **Wizards** tab, click the **Virtual Identity Wizard**.

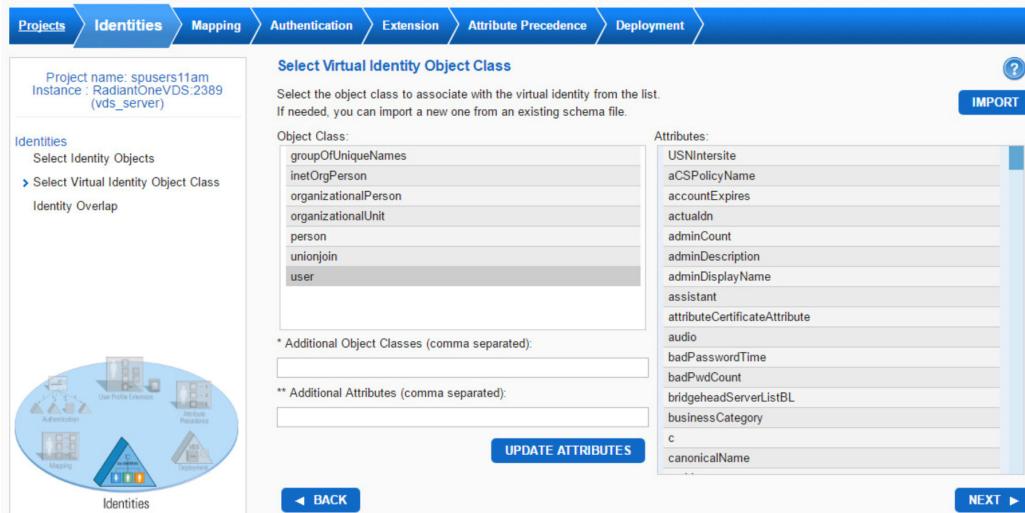


- 1546  
1547 2. Click **Next**.  
1548 3. Click **New** and enter a project name (e.g., spusers) and click **Next**.  
1549 4. If you do not already have the schemas extracted from the data sources (or even data sources  
1550 defined), use the **+** button to do so. The schema objects selected must be the ones associated  
1551 with the user entries in the backends (e.g., InetOrgPerson for the LDAP, and user for AD). For  
1552 more information, including exact steps on this process, see the *RadiantOne System Admin*

- 1553                  *Guide.*
- 1554        5. After connections to the backends are established and the schemas have been extracted, the drop-down list will 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.”
- 1555
- 1556
- 1557        6. Create the Selected identity objects shown below with the user schema from the AD backend and the inetOrgPerson from the openLDAP backend.
- 1558



- 1559
- 1560        7. Click **Next**.
- 1561        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.
- 1562
- 1563
- 1564



- 1565
- 1566        9. Click **Next**.
- 1567        10. Select **Yes**. Click **Next**.

Project name: spusers11am  
Instance : RadiantOneVDS:2389  
(vds\_server)

Identities  
Select Identity Objects  
Select Virtual Identity Object Class  
Identity Overlap

Identity Overlap  
Do you have common users existing in more than one of the identity sources selected?

YES  
 NO

1568  
1569

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

Define correlation key

RDN Name of your identities:

For each identity object, define the logic for building a unique identifier.  
Entries that have the same correlation key value will be merged into one unified entry.

Identity object	Correlation key
o_proxy_ad.user	✓ cn=employeeNumber
o_proxy_opendap.inetOrgPerson	✓ cn=employeeNumber

1570  
1571  
1572

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

Define correlation key for 'o\_proxy\_ad.user'

Expression:

ATTRIBUTES    FUNCTIONS    CONSTANT    VALIDATE

1573  
1574  
1575

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

Define correlation key

RDN Name of your identities:

For each identity object, define the logic for building a unique identifier.  
Entries that have the same correlation key value will be merged into one unified entry.

Identity object	Correlation key
o_proxy_ad.user	✓ cn=employeeNumber
o_proxy_opendap.inetOrgPerson	✓ cn=employeeNumber

1576  
1577  
1578

- 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.

**Define Attribute Mappings**

Map the object attributes to the virtual identity attributes for each identity object.

Identity Object: o\_proxy\_ad.user

Source attribute	map to	Virtual identity attribute
USNIntersite	USNIntersite	
aCSPolicyName	aCSPolicyName	
accountExpires	accountExpires	
actualdn	actualdn	
adminCount	adminCount	
adminDescription	adminDescription	
adminDisplayName	adminDisplayName	
assistant	assistant	
attributeCertificateAttribute	attributeCertificateAttribute	
audio	audio	
badPasswordTime	badPasswordTime	
badPwdCount	badPwdCount	
bridgeheadServerListBL	bridgeheadServerListBL	
businessCategory	businessCategory	
c		

**BACK** **NEXT**

1579  
1580

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

**Define Attribute Mappings**

Map the object attributes to the virtual identity attributes for each identity object.

Identity Object: o\_proxy\_opendap.inetOrgPerson

Source attribute	map to	Virtual identity attribute
actualdn	dynamicCLAPServer	
audio	employeeID	
businessCategory	employeeNumber	
carLicense	employeeType	
cn	extensionName	
departmentNumber	fRSMemberReferenceBL	
description	fSMORoleOwner	
destinationIndicator	facsimileTelephoneNumber	
displayName	flags	
employeeNumber	fromEntry	
employeeType	frsComputerReferenceBL	
facsimileTelephoneNumber	generationQualifier	
givenName	givenName	
homePhone	groupMembershipSAM	
homePostalAddress	userPriority	
initials		

**BACK** **NEXT**

1581  
1582  
1583  
1584

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**.

**Identification**

Select how you would like to identify the users.

Check the virtual identity attributes below to mark them as login attributes:

- uSNLastObjRemoved
- uSNLastObjRem
- uSNSource
- uid
- unicodePwd
- url
- userAccountControl

1585  
1586  
1587

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

1588  
1589**18. Do not select Join Objects. Click Next.**

**Credential checking strategy**

When the same identity appears in more than one source, define the bind order for credential checking.

Enabled	Order	Name
<input checked="" type="checkbox"/>	1	o_proxy_ad.user
<input checked="" type="checkbox"/>	2	o_proxy_opendap.inetOrgPerson

**Select Join Objects**

Select a schema, and select the join objects.  
These objects will be used to extend your profile.

Schema: ad schemas ( Ldap )

Selected Join Objects:

inetOrgPerson  
person  
user

Starting point: DC=AcmeFinancial,DC=com

BACK NEXT

1590  
1591  
1592**19. You can set each attribute precedence for any attributes that have mappings from multiple objects. Select the employeeNumber attribute. Click PRECEDENCE.**

**Virtual Identity Attributes**

The following attributes will appear in your virtual identity.

For attributes that have mappings from multiple objects, you can set up an attribute precedence.

**PRECEDENCE**

Attributes

<input type="radio"/> dynamicLDAPServer	<input type="checkbox"/>
<input type="radio"/> employeeID	<input type="checkbox"/>
<input checked="" type="radio"/> employeeNumber	<input type="checkbox"/>
<input type="radio"/> employeeType	<input type="checkbox"/>
<input type="radio"/> extensionName	<input type="checkbox"/>

1593  
1594**20. Give AD the highest priority. Click O****Attribute mappings:**Virtual identity attribute: **employeeNumber**

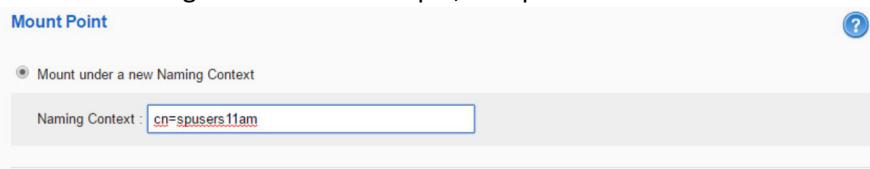
Identity Origin	Attribute from Origin	Priority
o_proxy_ad.user	employeeNumber	1 - HIGHEST ▾
o_proxy_opendap.inetOrgPerson	employeeNumber	3 - NORMAL ▾

**Warning:** The runtime processes the priority in 2 steps: the identities origins (union) then the extension origins (joins). The highest priority set on the union is going to be processed and compared at runtime with the priority set on each join.

OK CANCEL

1595  
1596**21. Click Next.**

1597 22. Name the naming context. For example, cn=spusers. Click **Next**.



1598  
1599 23. Select **Yes, I want a Periodic Cache Refresh**. Click **Next**.

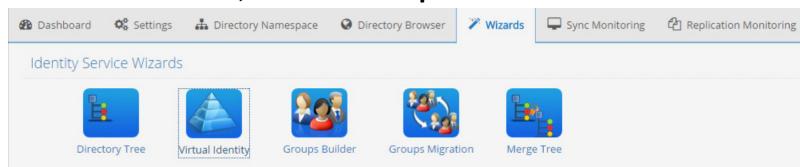


1600  
1601 24. Define the refresh interval. Click **Next**.

1602 25. Click **Initialize Cache Now**. Click **Finish**.

1603 Follow these steps to configure the groups for SharePoint:

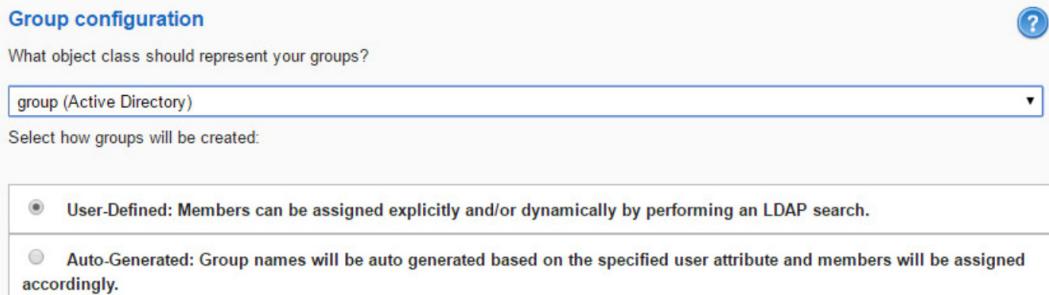
1604 1. On the **Wizards** tab, click the **Groups Builder Wizard**.



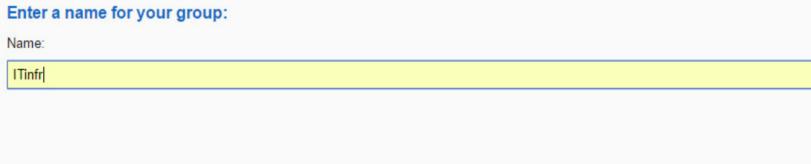
1605  
1606 2. Click **Next**.

1607 3. Name the project. Click **Next**.

1608 4. From the drop-down menu select **group (Active Directory)**. Select **User-Defined**. Click **Next**. For  
1609 more information on user-defined and auto-generated group, see the *RadiantOne FID System*  
1610 *Admin Guide*.



1611  
1612 5. Select **New Group**. Name the group ITinfr. Click **Next**.



1613  
1614 6. Repeat Step 5. Name the group Operations.

1615 7. Select the first Group. Click **Define Dynamic Members**.

**Define your groups**

Either create a new group or select a group and choose a method for adding members.

<b>NEW GROUP</b>	<b>DELETE GROUP</b>
<b>Group</b>	<b>Membership</b>
<input checked="" type="radio"/> ITinfr	<b>Manage Individual Members</b>
<input type="radio"/> Operations	<b>Define Dynamic Members</b>
<small>o=spusers11am; SUBTREE; (&amp; (objectclass=person) (actualdn=*,OU=ITinfr,*))</small>	
<small>🔍 🖍️ 🗑️</small>	

- 1616  
1617 8. Choose the naming context created in Step 23 of using the Virtual Identity Wizard. Type in the  
1618 following in the filter field: (& (objectclass=person) (actualdn=\*,OU=ITinfr,\*)). Select  
1619 **Sub-Tree**. Click **Next**.

**Define who belongs to the group 'ITinfr'**

Base DN:

CHOOSE

Filter:

One Level     Sub-Tree

PREVIEW

- 1620  
1621 9. Repeat Steps 7 and 8 with the following filter: (& (objectclass=person) (actualdn=\*,OU=Op-  
1622 erations,\*)).  
1623 10. Click **Next**.

**Define your groups**

Either create a new group or select a group and choose a method for adding members.

<b>NEW GROUP</b>	<b>DELETE GROUP</b>
<b>Group</b>	<b>Membership</b>
<input type="radio"/> ITinfr	
<input checked="" type="radio"/> Operations	<b>Manage Individual Members</b>
<small>o=spusers11am; SUBTREE; (&amp; (objectclass=person) (actualdn=*,OU=Operations,*))</small>	
<small>🔍 🖍️ 🗑️</small>	

- 1624  
1625 11. Enter a naming context to mount under. For example, cn= spgroups. Click **Next**.

**Mount Point**

Mount under a new Naming Context

Naming Context :

- 1626  
1627 12. Select **Yes, I want a Periodic Cache Refresh**. Click **Next**.

**Define a cache**

Do you want to use a cache?

<input type="radio"/> NO
<input checked="" type="radio"/> YES, I want a Periodic Cache Refresh
<input type="radio"/> YES, I want a Real Time Cache Refresh

If you want to use your own storage, do not set up the cache in the Wizard (choose NO), and configure your cache in the Control Panel (Directory Namespace tab) once the Wizard is complete.

- 1628  
1629 13. Define the refresh interval. Click **Next**.  
1630 14. Click **Initialize Cache Now**. Click **Finish**.

## 2.6.7 Scripts

1632 Two PowerShell scripts are scheduled to run on regular intervals on RadiantOne VDS server. The goal of  
1633 these scripts is to determine if the virtual directory server (RadiantOne VDS) and the RACF directory  
1634 server are online or offline. The first script determines if RadiantOne VDS is online or offline and writes  
1635 the corresponding status message to a local file being monitored by Splunk. The second script, which  
1636 also runs on the RadiantOne VDS server, determines if the Vanguard RACF directory is reachable and  
1637 writes corresponding offline or online messages to a local file also being monitored by Splunk.

```
1638 2.6.8 Script: RadiantOnlineStatus.ps1
1639 #This script checks determines if this server is online or offline
1640 #If gateway route exists and VDS server is running, the script will
1641 #output the current time, hostname, status and previous time (last
1642 #time it wrote to output file)
1643 #Check if gateway route exists and if the VDS service is running
1644 if ((Get-Netroute 0.0.0.0/0) -And (Get-Process vdsserver))
1645 {
1646     #Store date in PrevTime variable
1647     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1648     #Check if prevtime-file.txt exists
1649     if (ls C:\scripts\Radiant\prevtime-file.txt)
1650     {
1651         #Place the contents of prevtime-file.txt in the PrevTime variable
1652         $PrevTime=Get-Content C:\scripts\Radiant\prevtime-file.txt
1653     }
1654     #Place the current date in CurrentTime
1655     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1656     #Overwrite the contents of prevtime-file.txt with the current date
1657     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy" > C:\scripts\Radiant\prevtime-
1658 file.txt
1659     $HostVar = hostname
1660     $Status = 'online'
1661     #Add the contents of the variables CurrentTime, HostVar, Status, PrevTime to
1662 Radiant-Status-Output.csv
1663     Add-Content C:\scripts\Radiant\Radiant-Status-Output.csv
1664     $CurrentTime','$HostVar','$Status','$PrevTime'
1665 }
1666 else
1667 {
1668     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1669     if (ls C:\scripts\Radiant\prevtime-file.txt)
1670     {
1671         $PrevTime=Get-Content C:\scripts\Radiant\prevtime-file.txt
1672     }
```

```
1673     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"  
1674     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy" > C:\scripts\Radian\prevtime-  
1675     file.txt  
1676     $HostVar = hostname  
1677     $Status = 'offline'  
1678     Add-Content C:\scripts\Radian\Radian-Status-Output.csv  
1679     $CurrentTime', '$HostVar', '$Status', '$PrevTime'  
1680 }
```

## 2.6.9 Script: VanguardOnlineStatus.ps1

```
1681 #Script checks if the RACF mainframe is online and outputs status messages to file  
1682  
1683  
1684 #Check if the RACF mainframe is reachable with pings  
1685  
1686 if (ping -n 3 172.17.212.10 | select-string "Reply from 172.17.212.10")  
1687 {  
1688     #Store date in PrevTime variable  
1689     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"  
1690     #Check if prevtime-file.txt exists  
1691     if (ls C:\scripts\Vanguard\prevtime-file.txt)  
1692     {  
1693         #Place the contents of prevtime-file.txt in the PrevTime variable  
1694         $PrevTime=Get-Content C:\scripts\Vanguard\prevtime-file.txt  
1695     }  
1696     #Place the current date in CurrentTime  
1697     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"  
1698     #Overwrite the contents of prevtime-file.txt with the current date  
1699     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy" > C:\scripts\Vanguard\prevtime-  
1700     file.txt  
1701     $HostVar = "VanguardMainframe.acmefinancial.com"  
1702     $Status = 'online'  
1703     Add-Content C:\scripts\Vanguard\VanguardServer-Output.csv  
1704     $CurrentTime', '$HostVar', '$Status', '$PrevTime'  
1705 }  
1706 else  
1707 {  
1708     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
```

```
1709     if (ls C:\scripts\Vanguard\prevtime-file.txt)
1710         {
1711             $PrevTime=Get-Content C:\scripts\Vanguard\prevtime-file.txt
1712         }
1713         $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1714         Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy" > C:\scripts\Vanguard\prevtime-
1715 file.txt
1716         $HostVar = "VanguardMainframe.acmefinancial.com"
1717         $Status = 'offline'
1718         Add-Content C:\scripts\Vanguard\VanguardServer-Output.csv
1719         $CurrentTime', '$HostVar', '$Status', '$PrevTime
1720     }
```

## 2.6.10 LDAPS Configuration

1722 RadiantOne VDS virtual directory service connects to the Active Directory, OpenLDAP, and RACF  
1723 backend directory servers and takes snapshots of the directory contents. Configuring LDAPS ensures  
1724 that this process is encrypted with SSL. To use LDAPS to make these connections, follow these steps:

- 1725 1. Copy the certificates of the backend directories to the RadiantOne VDS virtual directory server.
- 1726 2. Import each certificate into the client trust store by opening the **Main Control Panel**.
- 1727 3. Click **Settings** tab > **Security** section > **Client Certificate Trust Store**.
- 1728 4. The certificates will be dynamically loaded into the Client Certificate Trust Store.
- 1729 5. Configure the backend connections to use LDAPS by going to the **Settings** tab.
- 1730 6. Click **Server Backend** > **LDAP Data Sources** > **Edit LDAP Data Source**.
- 1731 7. Check the **SSL** box and type **636** into the **Port** text box.

## 2.7 SharePoint

1733 SharePoint is a web-based, collaborative platform. SharePoint is primarily used as a document  
1734 management and storage system. It also supports workflow and applications.

### 2.7.1 How It's Used

1736 SharePoint 2013 is used as the web application to demonstrate the capability of the Access Rights  
1737 Management example solution.

### 2.7.2 Virtual Machine Configuration

1739 The SharePoint virtual machine is configured as follows:

- 1740 ▪ Ubuntu Linux 16.04 LTS
- 1741 ▪ 4 CPU cores
- 1742 ▪ 32GB of RAM
- 1743 ▪ 2 NICs

1744     ▪ 120GB of storage

1745 **Network Configuration (Interface 1)**

1746 IPv4 Manual

1747 IPv6 Disabled

1748 IP Address: 192.168.17.113

1749 Netmask: 255.255.255.0

1750 Gateway: 192.168.17.1

1751 DNS Name Servers: 192.168.19.10

1752 DNS-Search Domains: acmefinancial.com

1753 **2.7.3 Prerequisites**

1754 See the Microsoft [online](#) documentation for hardware and software prerequisites.

1755 **2.7.4 Installing SharePoint 2013**

1756 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](https://technet.microsoft.com/en-us/library/ms143219(v=sql.110).aspx)

1759 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>

1762 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>

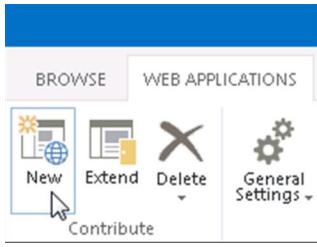
1766 **2.7.5 Configuring SharePoint**

1767 SharePoint must be integrated with the Radiant Logic Virtual Directory using Forms-Based

1768 Authentication. To integrate with the VD, complete the following steps:

1769 1. Open the SharePoint Central Administration Console, log in with your admin user, and click **Application Management**.

1771 2. Below the **Web Applications** section, click on **Manage Web Applications**.



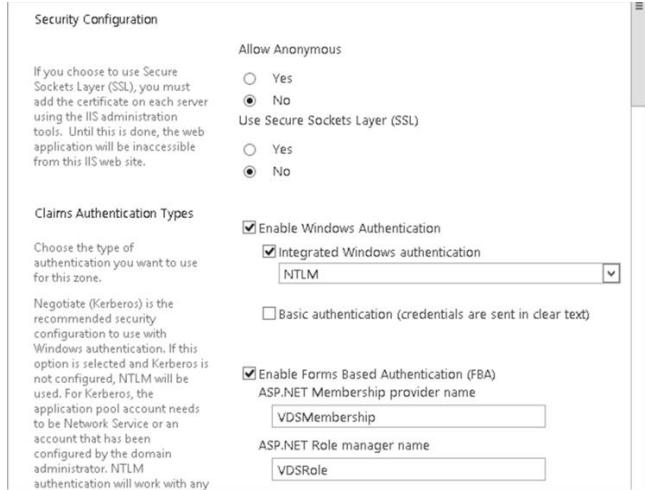
1772 3. Click the **New** button.

1773 4. You can choose to create a new IIS website and set a unique port.

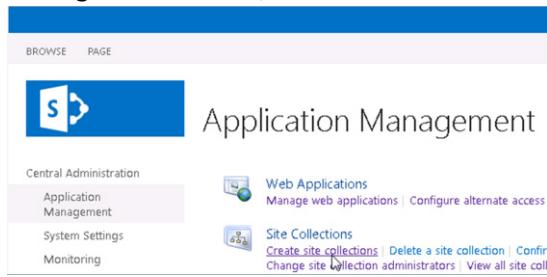
1775 Typically, you should accept the default path.

1776 5. In the Security Configuration section, you can leave the default options (Allow Anonymous=No, Use SSL=No).

- 1778        6. In the Claims Authentication Types section, check the option to **Enable Forms Based**  
 1779        **Authentication (FBA).**
- 1780        7. Enter a unique name for the ASP.NET Membership provider name and ASP.NET Role manager  
 1781        name.



- 1782        8. Leave the default sign-in page option selected.
- 1783        9. In the Public URL section, leave the default URL and Zone.
- 1784        10. In the Application Pool section, you can choose to “Create new application pool” and choose  
 1785        the “Predefined” option for the security account. Select the **Network Service** predefined  
 1786        option.
- 1787        11. Leave the default values for the Database Name and Authentication, Failover Server, Search  
 1788        Server, Service Application Connections, and Customer Experience Improvement Program  
 1789        sections.
- 1790        12. Click **OK** to create the new site.
- 1791        13. Because this is a new site, you will also need to setup a Site Collection. In the Application  
 1792        Management section, click **Create Site Collections**.



- 1794        14. Make sure your application shows in the Web Application parameter (if not, click in the drop-  
 1795        down list to select a new one). Enter a title description and web site address and choose a  
 1796        template.

1798

Create Site Collection

**Central Administration**

- Application Management
- System Settings
- Monitoring
- Backup and Restore
- Security
- Upgrade and Migration
- General Application Settings
- Apps
- Configuration Wizards

**Web Application**

To create a new web application go to [New Web Application page](#).

**Title and Description**

Type a title and description for your new site. The title will be displayed on each page in the site.

**Title:** VGS Team Site

**Description:** [Empty]

**Web Site Address**

Specify the URL name and URL path to create a new site, or choose to create a site at a specific path.  
To add a new URL Path go to the [Define Managed Paths page](#).

**URL:** http://demo-empty.sharepoint.com:48888 [New] [Delete]

**Template Selection**

Select experience version: 2013

Select a template: Collaboration Enterprise Custom

**Team Site** (selected)

Blog  
Developer Site  
Project Site  
Community Site

1799  
1800

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

**Template Selection**

Select experience version: 2013

Select a template: Collaboration Enterprise Publishing Custom

**Team Site** (selected)

Blog  
Developer Site  
Project Site  
Community Site

A place to work together with a group of people.

**Primary Site Collection Administrator**

Specify the administrator for this site collection. Only one user login can be provided; security groups are not supported.

User name: DEMO-EMPTY\administrator

**Secondary Site Collection Administrator**

Optionally specify a secondary site collection administrator. Only one user login can be provided; security groups are not supported.

User name: DEMO-EMPTY\administrator

**Quota Template**

Select a predefined quota template to limit resources used for this site collection.

To add a new quota template, go to the [Manage Quota Templates page](#).

Select a quota template: No Quota

Storage limit: Number of invited users:

1801

## 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 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 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.

```
<system.web>
<membership defaultProvider="i">
<providers>
<clear/>
```

```
1814 <add name="i"
1815 type="Microsoft.Sharepoint.Administration.Claims.SPClaimsAuthMembershipProvider,
1816 Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
1817 PublicKeyToken=71e9bce111e9429c" />
1818 <add name="VDSMembership"
1819 type="Microsoft.Office.Server.Security.LdapMembershipProvider,
1820 Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
1821 PublicKeyToken=71e9bce111e9429c"
1822     server="192.168.14.111"
1823     port="2389"
1824     useSSL="false"
1825     connectionUsername="cn=Directory Manager"
1826     connectionPassword="Fsarm@nccoel"
1827     useDNAttribute="false"
1828     userDNAttribute="distinguishedName"
1829     userNameAttribute="uid"
1830     userContainer="o=spusers11am"
1831     userObjectClass="user"
1832     userFilter="(ObjectClass=user)"
1833     scope="Subtree"
1834     otherRequiredUserAttributes="sn,givenname,cn,employeeNumber"/>
1835 </providers>
1836 </membership>
1837 <roleManager defaultProvider="c" enabled="true" cacheRolesInCookie="false" >
1838 <providers>
1839 <clear/>
1840 <add name="c"
1841 type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthRoleProvider,
1842 Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
1843 PublicKeyToken=71e9bce111e9429c" />
1844 <add name="VDSRole"
1845 type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
1846 Version=15.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
1847     server="192.168.14.111"
1848     port="2389"
1849     useSSL="false"
1850     groupContainer="o=spgroups11am"
1851     groupNameAttribute="cn"
```

```
1852      groupNameAlternateSearchAttribute="cn"
1853      groupMemberAttribute="member"
1854      userNameAttribute="uid"
1855      useUserDNAttribute="false"
1856      userContainer="o=spusers11am"
1857      dnAttribute="distinguishedName"
1858      groupFilter="(ObjectClass=group)"
1859      userFilter="(ObjectClass=user)"
1860      scope="Subtree" />
1861  </providers>
1862  </roleManager>
1863  </system.web>
```

1864 SharePoint Central Admin web config file is located at *C:\inetpub\wwwroot\wss\VirtualDirectories\<port the central admin is on>*.

1866 There is a default membership provider and a default role provider in the web.config file. Do not change  
1867 them. The names of the new membership provider and role manager that get added into the web.config  
1868 file must match the names set in the Forms Based configuration for the web application.

1869 Modify the file to include the following xml code in the <system.web> section:

```
1870  <membership defaultProvider="i">
1871    <providers>
1872      <clear />
1873      <add name="i"
1874        type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthMembershipProvider,
1875        Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
1876        PublicKeyToken=71e9bce11e9429c" />
1877      <add name="VDSMembership"
1878        type="Microsoft.Office.Server.Security.LdapMembershipProvider,
1879        Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
1880        PublicKeyToken=71e9bce11e9429c"
1881        server="192.168.14.111"
1882        port="2389"
1883        useSSL="false"
1884        connectionUsername="cn=Directory Manager"
1885        connectionPassword="Fsarm@nccoel"
1886        useDNAttribute="false"
1887        userDNAttribute="distinguishedName"
```

```
1888      userNameAttribute="uid"
1889      userContainer="o=spusers11am"
1890      userObjectClass="user"
1891      userFilter="(ObjectClass=user) "
1892      scope="Subtree"
1893      otherRequiredUserAttributes="sn,givenname,cn,employeeNumber"/>
1894  </providers>
1895 </membership>
1896 <roleManager defaultProvider="c" enabled="true" cacheRolesInCookie="false">
1897 <providers>
1898 <clear />
1899 <add name="c"
1900 type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthRoleProvider,
1901 Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
1902 PublicKeyToken=71e9bce111e9429c" />
1903 <add name="VDSRole"
1904 type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
1905 Version=15.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
1906     server="192.168.14.111"
1907     port="2389"
1908     useSSL="false"
1909     groupContainer="o=spgroups11am"
1910     groupNameAttribute="cn"
1911     groupNameAlternateSearchAttribute="cn"
1912     groupMemberAttribute="member"
1913     userNameAttribute="uid"
1914     useUserDNAttribute="false"
1915     userContainer="o=spusers11am"
1916     cacheDurationInMinutes="0"
1917     dnAttribute="distinguishedName"
1918     groupFilter="(ObjectClass=group) "
1919     userFilter="(ObjectClass=user) "
1920     scope="Subtree" />
1921 </providers>
1922 </roleManager>
```

1923 SharePoint Web Application web config is located at *C:\inetpub\wwwroot\wss\VirtualDirectories\<port*  
1924 *the application is on>*.

1925 There is a default membership provider and a default role provider in the web.config file. Do not change  
1926 them. The names of the new membership provider and role manager that get added into the web.config  
1927 file must match the names set in the Forms Based configuration for the web application.

1928 Modify the file to include the following xml code in the <system.web> section:

```
1929 <roleManager enabled="true" defaultProvider="AspNetWindowsTokenRoleProvider">
1930   <providers>
1931     <add name="VDSRole"
1932       type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
1933       Version=15.0.0.0, Culture=neutral,
1934       PublicKeyToken=71e9bce111e9429c"
1935       server="192.168.14.111"
1936       port="2389"
1937       useSSL="false"
1938       groupContainer="o=spgroups11am"
1939       groupNameAttribute="cn"
1940       groupNameAlternateSearchAttribute="cn"
1941       groupMemberAttribute="member"
1942       userNameAttribute="uid"
1943       dnAttribute="distinguishedName"
1944       groupFilter="(ObjectClass=group)"
1945       userFilter="(ObjectClass=person)"
1946       scope="Subtree" />
1947   </providers>
1948 </roleManager>
1949 <membership>
1950   <providers>
1951     <add name="VDSMembership"
1952       type="Microsoft.Office.Server.Security.LdapMembershipProvider,
1953       Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
1954       PublicKeyToken=71e9bce111e9429c"
1955       server="192.168.14.111"
1956       port="2389"
1957       useSSL="false"
```

```
1958      connectionUsername="cn=Directory Manager"
1959      connectionPassword="Fsarm@nccoel"
1960      useDNAttribute="false"
1961      userDNAttribute="distinguishedName"
1962      userNameAttribute="uid"
1963      userContainer="o=spusers11am"
1964      userObjectClass="person"
1965      userFilter="(ObjectClass=person)"
1966      scope="Subtree"
1967      otherRequiredUserAttributes="sn,givenname,cn"/>
1968  </providers>
1969  </membership>
1970  </system.web>
```

1971 To leverage RadiantOne Federated Identity for the SharePoint people picker, add the following line in  
1972 the <PeoplePickerWildcards> section of the web.config files for the SharePoint site and the Central Ad-  
1973 min (where VDSMembership is the name of the custom membership provider used):

```
1974 <add key="VDSMembership" value="*" />
1975 <PeoplePickerWildcards> <clear />
1976 <add key="AspNetSqlMembershipProvider" value="%" />
1977 <add key="VDSMembership" value="*" /> </PeoplePickerWildcards>
```

## 2.8 Splunk

1979 Splunk is a Security Information and Event Management system that allows for the collection and  
1980 parsing of logs and data from multiple systems.

### 2.8.1 How It's Used

1982 Splunk can receive data from a plethora of different sources. The most reliable option is installing  
1983 Splunk's "Universal Forwarder" on each system you want to collect data from. Other options include  
1984 syslogs, file and directory monitoring, network events, and more. Once data has been collected by  
1985 Splunk, it can then be parsed and displayed using prebuilt rules or custom criteria.

### 2.8.2 Installation

1987 Note: You will need a Splunk account to download Splunk Enterprise. The account is free and can be set  
1988 up at [https://www.splunk.com/page/sign\\_up](https://www.splunk.com/page/sign_up).

1989 Download Splunk Enterprise from [https://www.splunk.com/en\\_us/download/splunk-enterprise.html](https://www.splunk.com/en_us/download/splunk-enterprise.html).  
1990 Splunk can be installed on Windows, Linux, Solaris, and Mac OS X. Each of these installation instructions  
1991 can be found at:

- 1992     ▪ Windows

- 1993     • GUI: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonWindows>
- 1994
- 1995     • Command line: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonWindowsviaCommandLine>
- 1996
- 1997
- 1998     ▪ Linux: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonLinux>
- 1999     ▪ Solaris: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonSolaris>
- 2000     ▪ 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.

```

2013 (index=main sourcetype="wineventlog:security" EventCode=5136 OR EventCode=4720) OR
2014 (index=sandbox sourcetype="alertstatictest" OR sourcetype="RadianSourceTest") OR
2015 (index=main sourcetype="openldap-outlog")|rex "givenName:(?P<FirstName>\w+)"|rex
2016 "sn:(?P<LastName>\w+)"|rex mode=sed "s// /g"|rex
2017 "changetype:(?P<RLICHANGETYPE>\w+)"|rex "employeeNumber:(?P<EmployeeNumber>\w+)"|rex
2018 "changetype:modify (?P<CHANGE>.+) "|rex "conn=\d+\$\\w+:cn=(?P<LDAP_UID>\w+\$\\w+)"|rex
2019 "A user account was (?P<RLICHANGETYPE>\w+)"|rex "A directory service object was
2020 (?P<RLICHANGETYPE>\w+)"|eval
2021 RLICHANGETYPE;if(RLICHANGETYPE=="modified","update",RLICHANGETYPE)|eval
2022 RLICHANGETYPE;if(RLICHANGETYPE=="created","insert", RLICHANGETYPE)|eval
2023 RLICHANGETYPE;if(RLICHANGETYPE=="add","insert",RLICHANGETYPE)|fields _time host
2024 checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
2025 RLICHANGETYPE employeeNumber givenName sn uid gidnumber RLICHANGES LDAP_UID LDAP_MSG
2026 AD_UID AD_MSG |rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex "\-create\(\):User:
2027 (?P<AD_UID>\w+\$)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.\w+\$\\w+\$\\w+)"|rex "\-
2028 create\(\):User: (?P<AD_MSG>\w+\$\\w+\$\\w+)"|rex
2029 "<RLICHANGETYPE> (?P<RLICHANGETYPE>\w+)"|rex
2030 "<RLICHANGES> (?P<RLICHANGES>.+) \</RLICHANGES>"|rex "employeeNumber:
2031 (?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
2032 (?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\$+)"|rex
2033 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## l: (?P<L>\w+)"|rex "## o:
2034 (?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
2035 "mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\$+\$*\$+)"|rex
2036 "\<givenName\> (?P<GivenName>\$+\$*\$+)\<\\givenName\>"|rex
2037 "\<sn\> (?P<SurName>\$+\$*\$+)\<\\sn\>"|rex
2038 "\<employeeNumber\> (?P<EmployeeNumber>\$+\$*\$+)\<\\employeeNumber\>"|table _time

```

```

2039 host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
2040 RLICHANGETYPE RLICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
2041 LDAPUserId |where (isnotnull(FirstName)) OR (isnotnull(RLICHANGES) OR
2042 (isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG))) OR isnotnull(RLICHANGETYPE)|eval
2043 F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce.LastName,SurName)|eval
2044 EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
2045 LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID) |table
2046 _time host checkStatus EmpNo F_Name L_Name RLICHANGETYPE RLICHANGES checkAuthFields
2047 LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLICHANGES;if(RLICHANGETYPE=="insert","New User
2048 Record",RLICHANGES)| eval LDAP_UID;if((isnull(LDAP_UID) AND host=="RadianOne
2049 VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
2050 AD_UID;if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
2051 RLICHANGES;if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2052 RLICHANGES;if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2053 RLICHANGES;if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2054 RLICHANGES;if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2055 UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host;if(host=="WIN-
2056 CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
2057 maxspan=120s|eval host1;if(Like(host,"%RadianOne VDS%"),"RadianOne VDS","NULL")|eval
2058 host2;if(Like(host, "%WIN%"),"AlertE","NULL")|eval Authority;if((host1=="RadianOne
2059 VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
2060 Authority;if((host1=="RadianOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
2061 |table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
2062 AD_UID ADCHANGETYPE|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE
2063 RLICHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority !="Not Legal"|eval
2064 CHANGES;if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
2065 CHANGETYPE=if(isnotnull(RLICHANGETYPE),RLICHANGETYPE,RLICHANGETYPE)|table _time host
2066 Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Not
2067 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:

```

2071 earliest="1/25/2017:00:00:00" latest="2/15/2017:00:00:00" index=sandbox
2072 sourcetype="alertstatictest" OR sourcetype="RadianSourceTest" |fields _time host
2073 checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
2074 RLICHANGETYPE employeeNumber givenName sn uid gidnumber RLICHANGES LDAP_UID LDAP_MSG
2075 AD_UID AD_MSG|rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex "\-create\(\):User:
2076 (?P<AD_UID>\w+\s)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.\w+\s\w+\s\w+)"|rex "\-
2077 create\(\):User: (?P<AD_MSG>\w+\s\w+\s\w+)"|rex
2078 "<RLICHANGETYPE> (?P<RLICHANGETYPE>\w+)"|rex
2079 "<RLICHANGES> (?P<RLICHANGES>.+) \</RLICHANGES>"|rex "employeeNumber:
2080 (?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
2081 (?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\$+)"|rex
2082 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## l: (?P<L>\w+)"|rex "## o:
2083 (?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
2084 "mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\$+\s*\$+)"|rex
2085 "\<givenName\> (?P<GivenName>\$+\s*\$+)\</givenName\>"|rex
2086 "\<sn\> (?P<SurName>\$+\s*\$+)\</sn\>"|rex
2087 "\<employeeNumber\> (?P<EmployeeNumber>\$+\s*\$+)\</employeeNumber\>"|table _time
2088 host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
2089 RLICHANGETYPE RLICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
2090 LDAPUserId|where (isnotnull(FirstName)) OR (isnotnull(RLICHANGES) OR
2091 (isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG)))|eval
2092 F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce.LastName,SurName)|eval
2093 EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
2094 LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID) |table

```

```

2095 _time host checkStatus EmpNo F_Name L_Name RLICHANGETYPE RLICHANGES checkAuthFields
2096 LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLICHANGES;if(RLICHANGETYPE=="insert","New User
2097 Record",RLICHANGES)| eval LDAP_UID;if((isnull(LDAP_UID) AND host=="RadiantOne
2098 VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
2099 AD_UID;if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
2100 RLICHANGES;if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2101 RLICHANGES;if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2102 RLICHANGES;if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2103 RLICHANGES;if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2104 UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host;if(host=="WIN-
2105 CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
2106 maxspan=120s|eval host1;if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
2107 host2;if(Like(host, "%WIN%"),"AlertE","NULL")|eval Authority;if((host1=="RadiantOne
2108 VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
2109 Authority;if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
2110 |table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
2111 AD_UID|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE RLICHANGES
2112 EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority !="Not Legal"|eval
2113 CHANGES;if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
2114 CHANGETYPE;if(isnotnull(RLICHANGETYPE),RLICHANGETYPE,RLICHANGETYPE)|table _time host
2115 Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|timechart span=2d
2116 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:

```

2120 index=sandbox sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest"|fields
2121 _time host checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId
2122 LDAPUserId RLICHANGETYPE employeeNumber givenName sn uid gidnumber RLICHANGES
2123 LDAP_UID LDAP_MSG AD_UID AD_MSG|rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex
2124 "\-create\(\):User: (?P<AD_UID>\w+\$s)"|rex "\-create\(\):User:
2125 (?P<LDAP_MSG>\w+\.\w+\$w+\$s\w+)"|rex "\-create\(\):User: (?P<AD_MSG>\w+\$s\w+\$s\w+)"
2126 |rex "<RLICHANGETYPE>(?P<RLICHANGETYPE>\w+)"|rex
2127 "<RLICHANGES>(?P<RLICHANGES>.+)\\</RLICHANGES>"|rex "employeeNumber:
2128 (?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
2129 (?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\$+)"|rex
2130 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## l: (?P<L>\w+)"|rex "## o:
2131 (?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
2132 "mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\$+\$*\$+)"|rex
2133 "\<givenName\>(?P<GivenName>\$+\$*\$+)\</givenName\>"|rex
2134 "\<sn\>(?P<SurName>\$+\$*\$+)\</sn\>"|rex
2135 "\<employeeNumber\>(?P<EmployeeNumber>\$+\$*\$+)\</employeeNumber\>"|table _time
2136 host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
2137 RLICHANGETYPE RLICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
2138 LDAPUserId|where (isnotnull(FirstName)) OR (isnotnull(RLICHANGES) OR
2139 (isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG)))|eval
2140 F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
2141 EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
2142 LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD.UserId,AD_UID) |table
2143 _time host checkStatus EmpNo F_Name L_Name RLICHANGETYPE RLICHANGES checkAuthFields
2144 LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLICHANGES;if(RLICHANGETYPE=="insert","New User
2145 Record",RLICHANGES)| eval LDAP_UID;if((isnull(LDAP_UID) AND host=="RadiantOne
2146 VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
2147 AD_UID;if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
2148 RLICHANGES;if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2149 RLICHANGES;if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2150 RLICHANGES;if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval

```

```

2151 RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2152 UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
2153 CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
2154 maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
2155 host2=if(Like(host, "%WIN%"),"AlertE","NULL")|eval Authority=if((host1=="RadiantOne
2156 VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
2157 Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
2158 |table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
2159 AD_UID|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE RLICHANGES
2160 EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority !="Not Legal"|eval
2161 CHANGES=if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
2162 CHANGETYPE=if(isnotnull(RLICHANGETYPE),RLICHANGETYPE,RLICHANGETYPE)|table _time host
2163 Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID |eval
2164 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.

```

2165 (index=main sourcetype="wineventlog:security" EventCode=5136 OR EventCode=4720) OR
2166 (index=sandbox sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest") OR
2167 (index=main sourcetype="openldap-outlog")|rex "givenName:(?P<FirstName>\w+)"|rex
2168 "sn:(?P<LastName>\w+)"|rex mode=sed "s;/;/ /g"|rex
2169 "changetype:(?P<RLICHANGETYPE>\w+)"|rex "employeeNumber:(?P<EmployeeNumber>\w+)"|rex
2170 "changetype:modify (?P<CHANGE>.+) "|rex "conn=\d+\s\w+\:cn=(?P<LDAP_UID>\w+\$\\w+)"|rex
2171 "A user account was (?P<RLICHANGETYPE>\w+)"|rex "A directory service object was
2172 (?P<RLICHANGETYPE>\w+)"|eval
2173 RLICHANGETYPE=if(RLICHANGETYPE=="modified","update",RLICHANGETYPE)|eval
2174 RLICHANGETYPE=if(RLICHANGETYPE=="created","insert", RLICHANGETYPE)|eval
2175 RLICHANGETYPE=if(RLICHANGETYPE=="add","insert",RLICHANGETYPE)|fields _time host
2176 checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
2177 RLICHANGETYPE employeeNumber givenName sn uid gidnumber RLICHANGES LDAP_UID LDAP_MSG
2178 AD_UID AD_MSG |rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex "\-create\(\):User:
2179 (?P<AD_UID>\w+\$)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.\w+\$\\w+\$\\w+)"|rex "\-
2180 create\(\):User: (?P<AD_MSG>\w+\$\\w+\$\\w+)" |rex
2181 "<RLICHANGETYPE> (?P<RLICHANGETYPE>\w+)"|rex
2182 "<RLICHANGES> (?P<RLICHANGES>.) \<\|/RLICHANGES\>"|rex "employeeNumber:
2183 (?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
2184 (?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\$+)"|rex
2185 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## l: (?P<L>\w+)"|rex "## o:
2186 (?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
2187 "mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\$+\$*\$+)"|rex
2188 "\<givenName\> (?P<GivenName>\$+\$*\$+)\<\|/givenName\>"|rex
2189 "\<sn\> (?P<SurName>\$+\$*\$+)\<\|/sn\>" |rex
2190 "\<employeeNumber\> (?P<EmployeeNumber>\$+\$*\$+)\<\|/employeeNumber\>" |table _time
2191 host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
2192 RLICHANGETYPE RLICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
2193 LDAPUserId |where (isnotnull(FirstName)) OR (isnotnull(RLICHANGES)) OR
2194 (isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG)) OR isnotnull(RLICHANGETYPE)|eval
2195 F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
2196 EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
2197 LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID) |table
2198 _time host checkStatus EmpNo F_Name L_Name RLICHANGETYPE RLICHANGES checkAuthFields
2199 LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLICHANGES=if(RLICHANGETYPE=="insert","New User
2200 Record",RLICHANGES)| eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
2201 VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval

```

```

2206 AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
2207 RLICHANGES=if(Like(LDAP_MSG,"%created%"), "New User Record",RLICHANGES)|eval
2208 RLICHANGES=if(Like(AD_MSG,"%created%"), "New User Record",RLICHANGES)|eval
2209 RLICHANGES=if(Like(LDAP_MSG,"%created%"), "New User Record",RLICHANGES)|eval
2210 RLICHANGES=if(Like(AD_MSG,"%created%"), "New User Record",RLICHANGES)|eval
2211 UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
2212 CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
2213 maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"), "RadiantOne VDS", "NULL")|eval
2214 host2=if(Like(host, "%WIN%"), "AlertE", "NULL")|eval Authority=if((host1=="RadiantOne
2215 VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
2216 Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
2217 |table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
2218 AD_UID ADCHANGETYPE|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE
2219 RLICHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority != "Not Legal"|eval
2220 CHANGES=if(isnotnull(RLICHANGES), RLICHANGES,RLICHANGES)|eval
2221 CHANGETYPE=if(isnotnull(RLICHANGETYPE), RLICHANGETYPE,RLICHANGETYPE)|table _time host
2222 Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Not
2223 Like(CHANGES, "%lastLogonTimestamp%")|table _time host Authority CHANGETYPE CHANGES
2224 EmpNo F_Name L_Name LDAP_UID AD_UID|where isnotnull(CHANGETYPE) AND ((Like(CHANGES,
2225 "%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.

```

2231 earliest=-24h sourcetype="radiant-status"|table _time CurrentTime Hostname Status|sort
2232 1 _time|eval SearchTime_Epoch=now()|eval CTime_Epoch=strptime(CurrentTime,"%a %b %d
2233 %H:%M:%S %Z %Y")|eval TimeDiff=(SearchTime_Epoch - CTime_Epoch)|eval Status=if(TimeDiff
2234 > 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.

```

2238 earliest=-12h (index=sandbox sourcetype="radiantsourcetest" ERROR) OR (index=main
2239 sourcetype=openldap-status1) OR (index=main sourcetype=AD-Status) OR
2240 (sourcetype="Vanguard-Status") OR (sourcetype="Radiant-Status") |rex "Exception taking
2241 snapshot. Entries in snapshot: 0 Error :com.rli.slapd.server.LDAPException:
2242 (?P<IPAddress>\d+\.\d+\.\d+\.\d+)"|rex "ERROR (?P<ConnectionStatus>\w+\s\w+)"|table
2243 _time CurrentTime PrevTime Hostname Status IPAddress ConnectionStatus|eval
2244 CTime=strptime(CurrentTime,"%a %b %d %H:%M:%S %Z %Y")|eval PTime=strptime(PrevTime,"%a
2245 %b %d %H:%M:%S %Z %Y")|eval TimeDiff=(CTime-PTime)|eval
2246 Hostname=if(IPAddress=="192.168.19.11", "openldap.acmefinancial.com", Hostname)|eval
2247 Hostname=if(IPAddress=="192.168.19.10", "ActiveDirectory.acmefinancial.com",
2248 Hostname)|eval Hostname=if(Hostname=="RadiantOne VDS", "RadiantOne
2249 VDS.acmefinancial.com", Hostname)|eval Hostname=if(Hostname=="ActiveDirectory",
2250 "ActiveDirectory.acmefinancial.com", Hostname)|eval
2251 Status=if(ConnectionStatus=="Connection error", "offline", Status)|where
2252 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

2256 <http://docs.splunk.com/Documentation/Splunk/6.5.3/Security/ConfigureSplunkforwardingtousesignedcertificates>.

## 2258 2.9 TDI ConsoleWorks

2259 ConsoleWorks is a product that provides a portal for remote access to devices, a logging facility with  
2260 advanced hashing and pattern matching features, and role-based access control for administrators.

### 2261 2.9.1 How It's Used

2262 ConsoleWorks provides a portal through which privileged users access directory servers and core  
2263 systems in the lab infrastructure. There are two primary types of access connectors that are configured.  
2264 The first is a console connector that is either an SSH or Telnet connection to an internal LAN system. The  
2265 other is a graphical user interface (GUI) connector that can be either through Remote Desktop Protocol  
2266 (RDP) or Virtual Network Computing (VNC). In this build, SSH was used for the console connections,  
2267 whereas RDP was used for the GUI connections.

2268 The ConsoleWorks Server sits on a separate subnet that is connected to the Internet via a virtual private  
2269 network. It is configured to allow connections initiated from the VPN, but it drops connections initiated  
2270 from the LAN.

2271 Additionally, ConsoleWorks maintains logs of what systems were accessed, the time of access, and by  
2272 whom. These logs are formatted and prepared for consumption by the Splunk indexer.

### 2273 2.9.2 Virtual Machine Configuration

2274 ConsoleWorks virtual machine is configured as follows:

- 2275     ■ CentOS 7.2.1511
- 2276     ■ 1CPU cor
- 2277     ■ 8GB of RAM
- 2278     ■ 2 NICs
- 2279     ■ 100GB of storage.

#### 2280 Network Configuration (LAN)

2281 IPv4 Manual  
2282 IPv6 Enabled  
2283 IP Address: 192.168.17.11  
2284 Netmask: 255.255.255.0  
2285 Gateway: 192.168.17.1  
2286 DNS Name Servers 192.168.19.10  
2287 DNS-Search Domains: acmefinancial.com

#### 2288 Network Configuration (WAN)

2289 IPv4 Manual  
2290 IPv6 Enabled

2291 IP Address: 10.33.50.164  
 2292 Netmask: 255.255.240.0

### 2293 2.9.3 Firewall Configuration

2294 Enter the following commands in sequence to allow traffic to ports 5176 and 22 ports only. The  
 2295 ConsoleWorks web service listens on port 5176.

- 2296 1. **firewall-cmd – zone=public – add-port=5176/tcp**
- 2297 2. **firewall-cmd – zone=public – add-port=22/tcp**

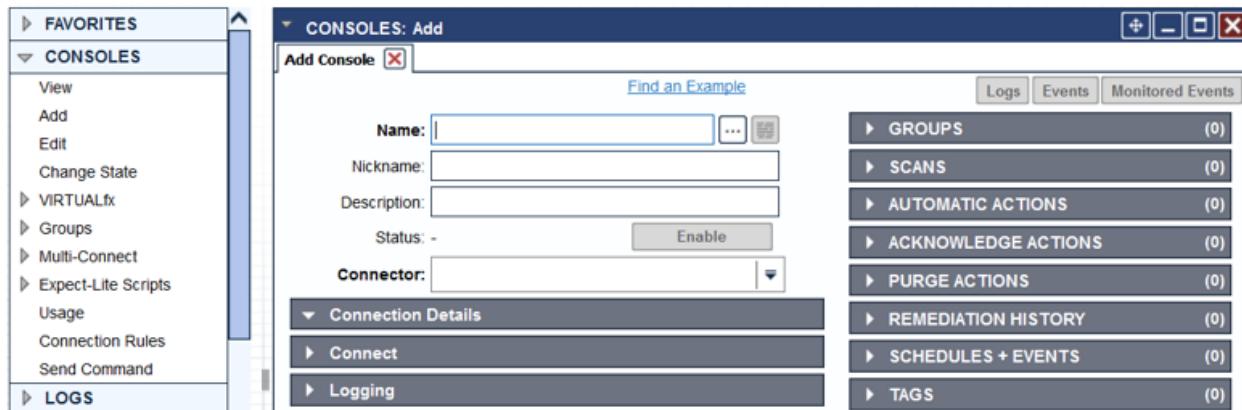
### 2298 2.9.4 Installation

2299 Installation for Windows, Linux, and Solaris systems can be found at  
 2300 <http://support.tditechnologies.com/tags/installation-guides>

### 2301 2.9.5 Console Connection Configuration

2302 To create a console connection:

- 2303 1. Click on **Consoles>Add**.
- 2304 2. Type in the name of the Console (for example, **OpenLDAPServer**).
- 2305 3. Choose the **Connector** type (for example, **SSH on Demand**).
- 2306 4. Click **Connection Details**. Check the **Exclusive Connect** checkbox.
- 2307 5. Type in the **Host IP**, **Port**, **Username**, and **Password** fields.
- 2308 6. Click **Save**.



### 2310 2.9.6 Graphical Gateway Configuration

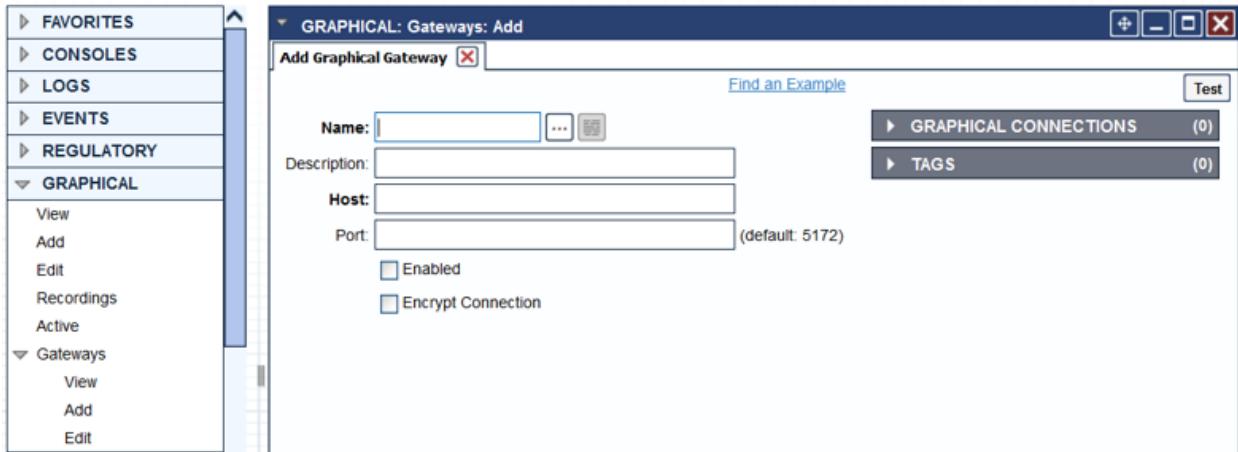
2311 A Graphical Gateway is required to make an RDP or VNC connection to a server.

2312 To configure a Graphical Gateway, you need to obtain and install the graphical gateway package from  
 2313 TDI Technologies Inc. The following steps describe installing and starting the service once the package is  
 2314 obtained.

```
2315 rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-version.rpm
2316 /opt/gui_gateway/install_local.sh
2317 /opt/ConsoleWorks/bin/cw_start <invocation name> (created during installation)
2318 service gui_gatewayd start
```

2319 Install the Graphical gateway:

- 2320 1. On the landing page on your ConsoleWorks server, click **GRAPHICAL>Gateways>Add**.  
 2321 2. Give it a name, then set **Host** as Localhost and **Port** as 5172.  
 2322 3. Check **Enabled** checkbox and click **Save**.  
 2323 4. Verify it works by clicking **Test** in the top-left corner.

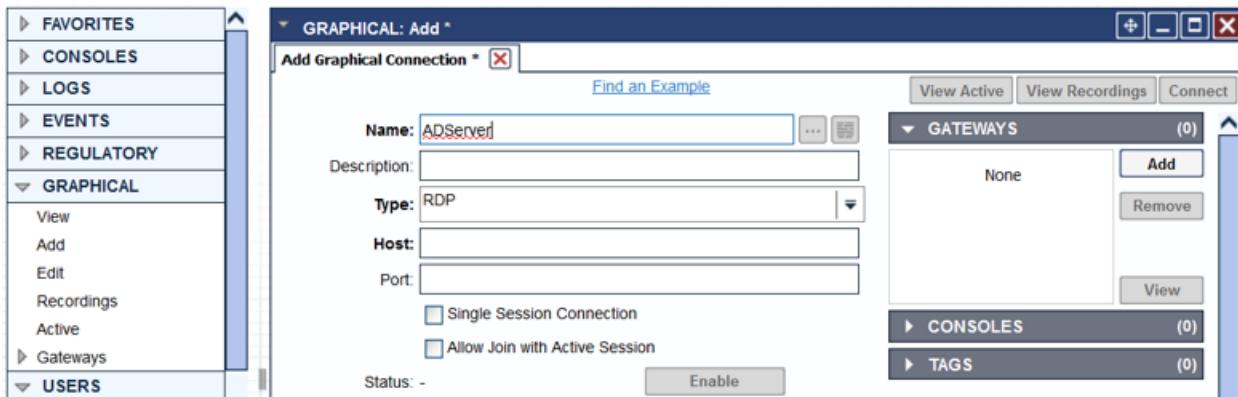


2324

### 2.9.7 Graphical Connection Configuration

2325 Configure the Graphical gateway:

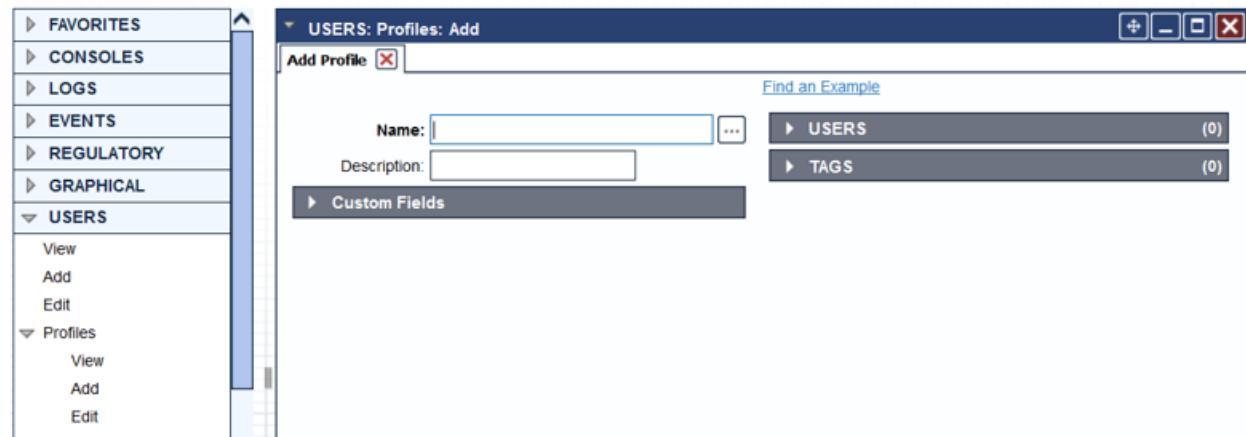
- 2326 1. On the landing page of your ConsoleWorks server, click **GRAPHICAL>Add**.  
 2327 2. Type in the name of the Graphical connection (for example, **ADServer**).  
 2328 3. Choose a protocol in the **Type** drop-down list (for example, **RDP**).  
 2329 4. Enter the name or IP address of the server in the **Host** field.  
 2330 5. Type in the port number in the **Port** field. Enter **3389** for RDP.  
 2331 6. Click **Save**.



2332

### 2.9.8 Profile Creation

- 2333 1. Click **USERS>Profiles>Add**.  
 2334 2. Type in the name of the profile in the **Name** field.  
 2335 3. Click **Save**.



2338

### 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.

**SECURITY: Access Control: View**

Order	Access Control Rule	Description	Enabled
48	COPY_CONSOLE_WRITE	Sample Console WRITE access	Y
49	COPY_CONSOLE_READ	Sample Console READ access	Y
50	COPY_CONSOLE_CONTROL	Sample Console CONTROL access	Y
100	NO_ARCH_NO_SPECIAL	Deny access to special Architect actions	Y
105	DENY_EVENTOCC_STATE_NEW_PURGE	DENY Purge access to Event State NEW	Y
110	ADMIN_CONTROL	Admin CONTROL access to EVERYTHING	Y
120	NO_CONTROL_NO_ACE	Deny Ace access if not Admin CONTROL	Y
130	NO_CONTROL_NO_USER	Deny User access if not Admin CONTROL	Y
140	NO_CONTROL_NO_PROFILE	Deny Profile access if not Admin CONTROL	Y
150	NO_CONTROL_NO_SYSTEM	Deny System Config access if not Admin CONTROL	Y
160	NO_CONTROL_NO_CONS_TAG	Deny Console-Tag association edit if not Admin CONTROL	Y
170	NO_CONTROL_NO_CMDCTRL_TAG	Deny CommandControl-Tag association edit if not Admin CC	Y
200	ADMIN_DELETE	Admin DELETE main access	Y
210	ADMIN_DELETE_CONSOLE	Admin DELETE access to Consoles	Y
220	ADMIN_WRITE	Admin WRITE main access	Y
230	ADMIN_WRITE_CONSOLE	Admin WRITE access to Consoles	Y
240	ADMIN_READ	Admin READ main access	Y
250	ADMIN_READ_CONSOLE	Admin READ access to Consoles	Y
300	DEF_NO_ADD-DEL_CONS	Default DENY Console create/delete	Y

2349

2350 To create a profile:

- 2351 1. In the **Allow or Deny** field, Select **ALLOW**.
- 2352 2. In the component **Type**, select **Console**.
- 2353 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.
- 2354 4. In the **Resource Selection** section, select the Console you want users associated with this profile to connect to. Select the **OpenLDAP** console.

**SECURITY: Access Control: Edit \***

**View Access Control Rules** **Edit Access Control Rule \***

**History**

**Name:** COPY\_CONSOLE\_CONTROL **Description:** Sample Console CONTROL access **Enabled:**  **Order:** 50 **Allow or Deny:** ALLOW **Audit Rule Usage:**  **Component Type:** Console

**TIME-FRAMES (0)**

**Profile Selection**

**Simple Basic Advanced Profiles**

DEFAULT	<input type="button" value="&lt;"/>	TESTPI	RADIANTLOGICPROFILE
RADIANTLOGICPROFILE	<input type="button" value="&gt;&gt;"/>	RADIAN	TESTPROFILE

**Resource Selection**

**Simple Basic Advanced Consoles**

**Selection:** - [Property\\_Console\\_Equals\\_OpenLDAP\\_<join>](#) + OPENLDAP

**Set As Default** **Save As...** **Delete** **Cancel** **Save**

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**.

**SECURITY: Access Control: View**

Order	Access Control Rule	Description	Enabled
99900	DEF_DOWNTIME_DENY	Default DENY Downtime	
99905	DEF_SSH_KEY_DENY	Default DENY SSH Key	Y
99907	DEF_TEMPLATE_DENY	Default DENY Template	Y
99913	DEF_BASELINE_DENY	Default DENY Baseline	Y
99915	DEF_SCHEDULER_DENY	Default DENY Schedule	Y
99917	DEF_REPORT_DENY	Default DENY Report	Y
99921	DEF_REGULATION_DENY	Default DENY Regulation	Y
99923	DEF_REGULATION_SET_DENY	Default DENY Regulation Set	Y
99925	DEF_REGULATORY_EVENT_DENY	Default DENY Regulatory Event	Y
99927	DEF_REGULATION_SEVERITY_DENY	Default DENY Regulation Severity	Y
99931	DEF_REGISTRATION_DENY	Default DENY Registration	Y
99933	DEF_CWSSHCLI_CONFIG_DENY	Default DENY CW SSH CLI Config	Y
99935	DEF_CWSCRIPT_DENY	Default DENY CWScript	Y
99940	ALLOW_COPY_DEF_GRAPHICAL_1	Default ALLOW Graphical Connection	Y
99941	DEF_GRAPHICAL_DENY	Default DENY Graphical Connection	Y
99943	DEF_GUIGATEWAY_DENY	Default DENY Graphical Gateway	Y
99990	DEF_CONSOLE_DENY	Default DENY Console	Y
99993	DEF_VIRTUAL_DENY	Default DENY Virtual Machine	Y
99995	DEF_MULTICONN_DENY	Default DENY Multi-Connect	Y
100000	DEF_AWARE	Default view	Y

2361

- 2362 1. To link an access control rule to a profile and a resource, first follow these steps:Edit this rule  
2363 and change the **Allow or Deny** field from DENY to **ALLOW**.  
2364 2. Change the Description to **Default ALLOW Graphical Connection**.  
2365 3. Ensure that the order number is lower than the Default DENY Graphical Connection rule  
2366 (DEF\_GRAPHICAL\_DENY).  
2367 4. Under Profile Selection, click the **Simple** tab and select “Is one of these Profiles.”  
2368 5. Select the profile of choice and make sure it appears on the right under Profiles.

**SECURITY: Access Control: Edit**

**View Access Control Rules**  **Edit Access Control Rule**

**History**

**Name:** ALLOW\_COPY\_DEF\_GRAPHICAL\_1

**Description:** Default ALLOW Graphical Connection

Enabled

**Order:** 99940

**Allow or Deny:** ALLOW

Audit Rule Usage

**Component Type:** Graphical Connection

**Profile Selection**

**Simple** **Basic** **Advanced** **Profiles**

Is one of these Profiles

All Profiles

**Profile**  **Select**

CONSOLE_MANAGER	<input type="button" value="&lt;"/>	TESTT/
DEFAULT	<input type="button" value="&gt;&gt;"/>	

**Resource Selection**

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.

**SECURITY: Access Control: Edit**

**View Access Control Rules** **Edit Access Control Rule**

**History**

**Name:** ALLOW\_COPY\_DEF\_GRAPHICAL\_1 **Description:** Default ALLOW Graphical Connection  
 Enabled **Order:** 99940 **Allow or Deny:** ALLOW  
 Audit Rule Usage **Component Type:** Graphical Connection

**Profile Selection**

**Resource Selection**

**Simple** **Basic** **Advanced** **Graphical Connections**

Is one of these Graphical Connections

All Graphical Connections

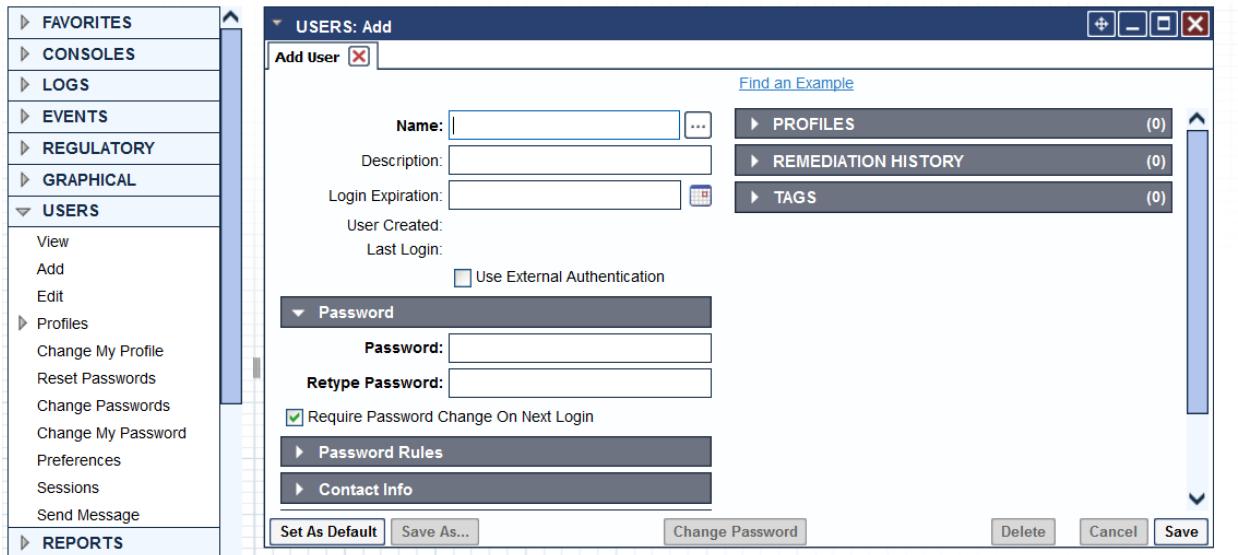
Graphical Connection	Select
ADTEST	/
RADIANTONEVDS	[>>]

**Set As Default** **Save As...** **Delete** **Cancel** **Save**

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.



2379

## 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 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 connection reporting script removes duplicate lines. The bash connection reporting script is scheduled using cron to run every minute using the following /etc/crontab configuration.

## 2.9.11 Cron Configuration: /etc/crontab

```

2388 SHELL=/bin/bash
2389 PATH=/sbin:/bin:/usr/sbin:/usr/bin
2390 MAILTO=root
2391 # For details see man 4 crontabs
2392 # Example of job definition:
2393 # .----- minute (0 - 59)
2394 # | .----- hour (0 - 23)
2395 # | | .----- day of month (1 - 31)
2396 # | | | .---- month (1 - 12) OR jan,feb,mar,apr ...
2397 # | | | | .--- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
2398 # | | | | |
2399 # * * * * * user-name command to be executed
2400 * * * * * root      /etc/cron.daily/bashconnectionreporting

```

## 2.9.12 Scripts: connectionreporting

```

2402 #!/usr/bin/python3.5
2403 # Script identifies ConsoleWorks users, connection times and their targets

```

```

2404 #import the OS module
2405 import os
2406 #Store the ConsoleWorks log directory in the "directory" variable
2407 directory = "/opt/ConsoleWorks/FSARM/log"
2408 #Change directory to the Log dir
2409 os.chdir(directory)
2410 #Iterate through files in log dir and look for strings shown in the
2411 #IF statements. Matching lines are written to file
2412 for file in os.listdir(directory):
2413     with open(file, 'r') as file_object:
2414         for line in file_object:
2415             if "CONWRKS Audit:: User:" in line:
2416                 with open('/var/log/connections.out','a') as outfile_object:
2417                     outfile_object.write(line)
2418             if "connecting" in line:
2419                 with open('/var/log/connections.out','a') as outfile_object:
2420                     outfile_object.write(line)
2421             if "disconnecting" in line:
2422                 with open('/var/log/connections.out','a') as outfile_object:
2423                     outfile_object.write(line)

```

### 2.9.13 Scripts: bashconnectionreporting

```

2425 #!/bin/bash
2426 #Calls python script that reads ConsoleWorks log files and outputs to
2427 #/var/log/connections.out
2428 /etc/cron.daily/connectionreporting
2429 #This line removes duplicate lines from the connections.out file and outputs them
2430 # to connections.log
2431 awk '!seen[$0]++' /var/log/connections.out > /var/log/connections.log

```

## 2.10 Network Firewall Configuration

2433 pfSense virtual devices were used as firewall routers for each subnet and were configured to restrict  
 2434 traffic as appropriate. The subnets listed below have critical services and resources that need to be  
 2435 accessed from devices external to the LAN. We have made the exact configuration used in each pfSense  
 2436 firewall available in XML format. This can be imported directly into another pfSense device. It is  
 2437 important to note that an IPSEC VPN connection was made to the offsite RACF LDAP directory server.  
 2438 The IPSEC VPN configuration was set up in the firewall for the backbone subnet.

2439   **2.10.1 Firewall Configuration for Backbone Subnet**

2440   <?xml version="1.0"?>

2441   <pfsense>

2442     <version>15.4</version>

2443     <lastchange/>

2444     <theme>pfsense\_ng</theme>

2445     <system>

2446       <optimization>normal</optimization>

2447       <hostname>pfsenseVLAN13</hostname>

2448       <domain>acmefinancial.com</domain>

2449       <group>

2450         <name>all</name>

2451         <description><! [CDATA[All Users] ]></description>

2452         <scope>system</scope>

2453         <gid>1998</gid>

2454         <member>0</member>

2455       </group>

2456       <group>

2457         <name>admins</name>

2458         <description><! [CDATA[System Administrators] ]></description>

2459         <scope>system</scope>

2460         <gid>1999</gid>

2461         <member>0</member>

2462         <priv>page-all</priv>

2463       </group>

2464       <user>

2465         <name>admin</name>

2466         <descr><! [CDATA[System Administrator] ]></descr>

2467         <scope>system</scope>

2468         <groupname>admins</groupname>

2469         <password>\$1\$dSJImFph\$GvZ7.1UbuWu.Yb8etC0re.</password>

2470         <uid>0</uid>

2471         <priv>user-shell-access</priv>

2472       </user>

```
2473      <nextuid>2000</nextuid>
2474      <nextgid>2000</nextgid>
2475      <timezone>America/New_York</timezone>
2476      <time-update-interval/>
2477      <timeservers>10.97.74.8</timeservers>
2478      <webgui>
2479          <protocol>http</protocol>
2480          <loginautocomplete/>
2481          <ssl-certref>5720a0502b277</ssl-certref>
2482          <dashboardcolumns>2</dashboardcolumns>
2483          <webguicss>pfsense.css</webguicss>
2484      </webgui>
2485      <disablesegmentationoffloading/>
2486      <disablelargereceiveoffloading/>
2487      <ipv6allow/>
2488      <powerd_ac_mode>hadp</powerd_ac_mode>
2489      <powerd_battery_mode>hadp</powerd_battery_mode>
2490      <powerd_normal_mode>hadp</powerd_normal_mode>
2491      <bogons>
2492          <interval>monthly</interval>
2493      </bogons>
2494      <language>en_US</language>
2495      <dns1gw>GW_WAN</dns1gw>
2496      <dns2gw>GW_WAN</dns2gw>
2497      <dns3gw>none</dns3gw>
2498      <dns4gw>none</dns4gw>
2499      <maximumstates/>
2500      <aliasesresolveinterval/>
2501      <maximumtableentries/>
2502      <maximumfrags/>
2503      <enablenatreflectionpurenat>yes</enablenatreflectionpurenat>
2504      <enablebinatreflection>yes</enablebinatreflection>
2505      <enablenatreflectionhelper>yes</enablenatreflectionhelper>
2506      <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>
```

```
2541          <gateway>VLAN2014</gateway>
2542          <descr/>
2543      </route>
2544      <route>
2545          <network>192.168.19.0/24</network>
2546          <gateway>VLAN2019</gateway>
2547          <descr/>
2548      </route>
2549      <route>
2550          <network>192.168.18.0/24</network>
2551          <gateway>VLAN2018</gateway>
2552          <descr/>
2553      </route>
2554      <route>
2555          <network>192.168.15.0/24</network>
2556          <gateway>VLAN2015</gateway>
2557          <descr/>
2558      </route>
2559      <route>
2560          <network>192.168.16.0/24</network>
2561          <gateway>VLAN2016</gateway>
2562          <descr/>
2563      </route>
2564      <route>
2565          <network>192.168.17.0/24</network>
2566          <gateway>VLAN2017</gateway>
2567          <descr/>
2568      </route>
2569      <route>
2570          <network>192.168.20.0/24</network>
2571          <gateway>VLAN2020</gateway>
2572          <descr/>
2573      </route>
2574      <route>
```

```
2575      <network>10.33.50.160/28</network>
2576      <gateway>VLAN2066</gateway>
2577      <descr><! [CDATA[Route to Vendor Net]]></descr>
2578      </route>
2579  </staticroutes>
2580  <dhcpd>
2581      <lan>
2582          <enable/>
2583          <range>
2584              <from>192.168.13.100</from>
2585              <to>192.168.13.150</to>
2586          </range>
2587          <failover_peerip/>
2588          <dhcpleaseinlocaltime/>
2589          <defaultleasetime/>
2590          <maxleasetime/>
2591          <netmask/>
2592          <dnsserver>192.168.19.10</dnsserver>
2593          <gateway/>
2594          <domain>acmefinancial.com</domain>
2595          <domainsearchlist>acmefinancial.com</domainsearchlist>
2596          <ddnsdomain/>
2597          <ddnsdomainprimary/>
2598          <ddnsdomainkeyname/>
2599          <ddnsdomainkey/>
2600          <mac_allow/>
2601          <mac_deny/>
2602          <tftp/>
2603          <ldap/>
2604          <nextserver/>
2605          <filename/>
2606          <filename32/>
2607          <filename64/>
2608          <rootpath/>
```

```
2609          <numberoptions/>
2610      </lan>
2611      <opt1>
2612          <enable/>
2613          <range>
2614              <from>192.168.14.100</from>
2615              <to>192.168.14.150</to>
2616          </range>
2617          <dhcpleaseinlocaltime/>
2618      </opt1>
2619      <opt2>
2620          <enable/>
2621          <range>
2622              <from>192.168.15.100</from>
2623              <to>192.168.15.150</to>
2624          </range>
2625          <dhcpleaseinlocaltime/>
2626      </opt2>
2627      <opt3>
2628          <enable/>
2629          <range>
2630              <from>192.168.16.100</from>
2631              <to>192.168.16.150</to>
2632          </range>
2633          <dhcpleaseinlocaltime/>
2634      </opt3>
2635  </dhcpd>
2636  <snmpd>
2637      <syslocation/>
2638      <syscontact/>
2639      <rocommunity>public</rocommunity>
2640  </snmpd>
2641  <diag>
2642      <ipv6nat>
```

```
2643          <ipaddr/>
2644      </ipv6nat>
2645  </diag>
2646  <bridge/>
2647  <syslog/>
2648  <nat>
2649      <outbound>
2650          <mode>automatic</mode>
2651      </outbound>
2652  <onetoone>
2653      <external>10.33.50.44</external>
2654      <descr><! [CDATA[mapping to 2020 pfsense firewall ]]></descr>
2655      <interface>wan</interface>
2656  <source>
2657      <address>192.168.13.20</address>
2658  </source>
2659  <destination>
2660      <any/>
2661  </destination>
2662  </onetoone>
2663  <onetoone>
2664      <external>10.33.50.42</external>
2665      <descr><! [CDATA[Mapping to PfSense firewall]]></descr>
2666      <interface>wan</interface>
2667  <source>
2668      <address>192.168.13.17</address>
2669  </source>
2670  <destination>
2671      <any/>
2672  </destination>
2673  </onetoone>
2674  <onetoone>
2675      <external>10.33.50.35</external>
2676      <descr><! [CDATA[Mapping to Splunk]]></descr>
```

```
2677             <interface>wan</interface>
2678             <source>
2679                 <address>192.168.17.11</address>
2680             </source>
2681             <destination>
2682                 <any/>
2683             </destination>
2684         </onetoone>
2685         <onetoone>
2686             <external>10.33.50.41</external>
2687             <descr><! [CDATA[Mapping to PfSense firewall]]></descr>
2688             <interface>wan</interface>
2689             <source>
2690                 <address>192.168.19.11</address>
2691             </source>
2692             <destination>
2693                 <any/>
2694             </destination>
2695         </onetoone>
2696         <onetoone>
2697             <external>10.33.50.36</external>
2698             <descr><! [CDATA[Mapping to Hytrust ESXi Server]]></descr>
2699             <interface>wan</interface>
2700             <source>
2701                 <address>192.168.20.12</address>
2702             </source>
2703             <destination>
2704                 <any/>
2705             </destination>
2706         </onetoone>
2707         <onetoone>
2708             <external>10.33.50.37</external>
2709             <descr><! [CDATA[NAT Mapping to RadiantOne VDS]]></descr>
2710             <interface>wan</interface>
```

```
2711          <source>
2712              <address>192.168.14.11</address>
2713          </source>
2714          <destination>
2715              <any/>
2716          </destination>
2717      </onetoone>
2718      <onetoone>
2719          <external>10.33.50.38</external>
2720          <descr><! [CDATA[NAT Mapping to Hytrust CloudControl VM] ]></descr>
2721          <interface>wan</interface>
2722      <source>
2723          <address>192.168.20.11</address>
2724      </source>
2725      <destination>
2726          <any/>
2727      </destination>
2728  </onetoone>
2729  <onetoone>
2730      <external>10.33.50.40</external>
2731      <descr><! [CDATA[Mapping to ActiveDirectory]]></descr>
2732      <interface>wan</interface>
2733  <source>
2734      <address>192.168.19.10</address>
2735  </source>
2736  <destination>
2737      <any/>
2738  </destination>
2739  </onetoone>
2740  <onetoone>
2741      <external>10.33.50.43</external>
2742      <descr><! [CDATA[VIP for ConsoleWorks -- Mapping to Internal
2743 Address]]></descr>
2744      <interface>wan</interface>
```

```
2745           <source>
2746               <address>192.168.17.11</address>
2747           </source>
2748           <destination>
2749               <any/>
2750           </destination>
2751       </onetoone>
2752   <onetoone>
2753       <external>10.33.50.45</external>
2754   <descr><! [CDATA[VIP for CentOSToAD-- Mapping to Internal
2755 Address]]></descr>
2756       <interface>wan</interface>
2757   <source>
2758       <address>192.168.19.30</address>
2759   </source>
2760   <destination>
2761       <any/>
2762   </destination>
2763 </onetoone>
2764 <onetoone>
2765       <external>10.33.50.46</external>
2766   <descr><! [CDATA[AlertEnterprise Enterprise Guardian]]></descr>
2767       <interface>wan</interface>
2768   <source>
2769       <address>192.168.17.114</address>
2770   </source>
2771   <destination>
2772       <any/>
2773   </destination>
2774 </onetoone>
2775 <rule>
2776   <source>
2777       <any/>
2778   </source>
```

```
2779          <destination>
2780              <network>wanip</network>
2781              <port>1322</port>
2782          </destination>
2783          <protocol>tcp</protocol>
2784          <target>192.168.13.130</target>
2785          <local-port>80</local-port>
2786          <interface>wan</interface>
2787          <descr><! [CDATA[Mapping to pfSense 192.168.13.130]]></descr>
2788          <associated-rule-id>nat_581795efbc2944.51341500</associated-rule-
2789      id>
2790          <created>
2791              <time>1477940719</time>
2792              <username>admin@192.168.13.139</username>
2793          </created>
2794          <updated>
2795              <time>1477940861</time>
2796              <username>admin@192.168.13.139</username>
2797          </updated>
2798      </rule>
2799      <rule>
2800          <source>
2801              <any/>
2802          </source>
2803          <destination>
2804              <address>10.33.50.41</address>
2805              <port>80</port>
2806          </destination>
2807          <protocol>tcp/udp</protocol>
2808          <target>192.168.19.11</target>
2809          <local-port>80</local-port>
2810          <interface>wan</interface>
2811          <descr><! [CDATA[Port forward to openldap; Add /phpldapadmin to
2812      address]]></descr>
```

```
2813          <associated-rule-id>nat_57bf0c96d083f4.07194849</associated-rule-
2814      id>
2815          <created>
2816              <time>1472138390</time>
2817              <username>admin@10.97.67.137</username>
2818          </created>
2819          <updated>
2820              <time>1473431620</time>
2821              <username>admin@10.97.67.134</username>
2822          </updated>
2823      </rule>
2824      <rule>
2825          <source>
2826              <any/>
2827          </source>
2828          <destination>
2829              <address>10.33.50.41</address>
2830              <port>22</port>
2831          </destination>
2832          <protocol>tcp/udp</protocol>
2833          <target>192.168.19.11</target>
2834          <local-port>22</local-port>
2835          <interface>wan</interface>
2836          <descr><! [CDATA[Port forward to openldap; ]]></descr>
2837      <associated-rule-id>nat_57f555406f2de3.01889708</associated-rule-
2838      id>
2839          <created>
2840              <time>1475695936</time>
2841              <username>admin@10.97.67.145</username>
2842          </created>
2843          <updated>
2844              <time>1475695966</time>
2845              <username>admin@10.97.67.145</username>
2846          </updated>
2847      </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>
```

```
2882      <local-port>22</local-port>
2883      <interface>wan</interface>
2884      <descr><! [CDATA[Splunk SSH ]]></descr>
2885      <associated-rule-id>nat_582ef78ed63d23.63868026</associated-rule-
2886      id>
2887      <updated>
2888          <time>1479473038</time>
2889          <username>admin@10.97.67.135</username>
2890      </updated>
2891      <created>
2892          <time>1479473038</time>
2893          <username>admin@10.97.67.135</username>
2894      </created>
2895  </rule>
2896  <rule>
2897      <source>
2898          <any/>
2899      </source>
2900      <destination>
2901          <address>10.33.50.42</address>
2902          <port>1314</port>
2903      </destination>
2904      <protocol>tcp/udp</protocol>
2905      <target>192.168.13.14</target>
2906      <local-port>80</local-port>
2907      <interface>wan</interface>
2908      <descr><! [CDATA[Port Forward to 192.168.13.14 Pf]]></descr>
2909      <associated-rule-id>nat_57c01545c247f0.43308393</associated-rule-
2910      id>
2911      <updated>
2912          <time>1472206149</time>
2913          <username>admin@10.97.67.135</username>
2914      </updated>
2915      <created>
2916          <time>1472206149</time>
```

```
2917             <username>admin@10.97.67.135</username>
2918         </created>
2919     </rule>
2920     <rule>
2921         <source>
2922             <any/>
2923         </source>
2924         <destination>
2925             <address>10.33.50.42</address>
2926             <port>1315</port>
2927         </destination>
2928         <protocol>tcp/udp</protocol>
2929         <target>192.168.13.15</target>
2930         <local-port>80</local-port>
2931         <interface>wan</interface>
2932         <descr><! [CDATA[Port Forward to 192.168.13.15 Pf]]></descr>
2933         <associated-rule-id>nat_57c0163d6e2de9.62906352</associated-rule-
2934 id>
2935     <updated>
2936         <time>1472206397</time>
2937         <username>admin@10.97.67.135</username>
2938     </updated>
2939     <created>
2940         <time>1472206397</time>
2941         <username>admin@10.97.67.135</username>
2942     </created>
2943     </rule>
2944     <rule>
2945         <source>
2946             <any/>
2947         </source>
2948         <destination>
2949             <address>10.33.50.42</address>
2950             <port>1316</port>
```

```
2951             </destination>
2952             <protocol>tcp/udp</protocol>
2953             <target>192.168.13.16</target>
2954             <local-port>80</local-port>
2955             <interface>wan</interface>
2956             <descr><! [CDATA[Port Forward to 192.168.13.16 Pf]]></descr>
2957             <associated-rule-id>nat_57c01682da98c4.72334719</associated-rule-
2958 id>
2959             <updated>
2960                 <time>1472206466</time>
2961                 <username>admin@10.97.67.135</username>
2962             </updated>
2963             <created>
2964                 <time>1472206466</time>
2965                 <username>admin@10.97.67.135</username>
2966             </created>
2967         </rule>
2968         <rule>
2969             <source>
2970                 <any/>
2971             </source>
2972             <destination>
2973                 <address>10.33.50.42</address>
2974                 <port>1317</port>
2975             </destination>
2976             <protocol>tcp/udp</protocol>
2977             <target>192.168.13.17</target>
2978             <local-port>80</local-port>
2979             <interface>wan</interface>
2980             <descr><! [CDATA[Port Forward to 192.168.13.17 Pf]]></descr>
2981             <associated-rule-id>nat_57c01787b4e891.75909166</associated-rule-
2982 id>
2983             <updated>
2984                 <time>1472206727</time>
2985                 <username>admin@10.97.67.135</username>
```

```
2986          </updated>
2987          <created>
2988              <time>1472206727</time>
2989              <username>admin@10.97.67.135</username>
2990          </created>
2991      </rule>
2992      <rule>
2993          <source>
2994              <any/>
2995          </source>
2996          <destination>
2997              <address>10.33.50.42</address>
2998              <port>1318</port>
2999          </destination>
3000          <protocol>tcp/udp</protocol>
3001          <target>192.168.13.18</target>
3002          <local-port>80</local-port>
3003          <interface>wan</interface>
3004          <descr><! [CDATA[Port Forward to 192.168.13.18 Pf]]></descr>
3005          <associated-rule-id>nat_57c017be3dfffa1.16882401</associated-rule-
3006      id>
3007          <updated>
3008              <time>1472206782</time>
3009              <username>admin@10.97.67.135</username>
3010          </updated>
3011          <created>
3012              <time>1472206782</time>
3013              <username>admin@10.97.67.135</username>
3014          </created>
3015      </rule>
3016      <rule>
3017          <source>
3018              <any/>
3019          </source>
```

```
3020      <destination>
3021          <address>10.33.50.42</address>
3022          <port>1319</port>
3023      </destination>
3024      <protocol>tcp/udp</protocol>
3025      <target>192.168.13.19</target>
3026      <local-port>80</local-port>
3027      <interface>wan</interface>
3028      <descr><! [CDATA[Port Forward to 192.168.13.19 Pf]]></descr>
3029      <associated-rule-id>nat_57c017e1e48d65.86612217</associated-rule-
3030 id>
3031      <updated>
3032          <time>1472206817</time>
3033          <username>admin@10.97.67.135</username>
3034      </updated>
3035      <created>
3036          <time>1472206817</time>
3037          <username>admin@10.97.67.135</username>
3038      </created>
3039  </rule>
3040  <rule>
3041      <source>
3042          <any/>
3043      </source>
3044      <destination>
3045          <address>10.33.50.42</address>
3046          <port>1320</port>
3047      </destination>
3048      <protocol>tcp/udp</protocol>
3049      <target>192.168.13.20</target>
3050      <local-port>80</local-port>
3051      <interface>wan</interface>
3052      <descr><! [CDATA[Port Forward to 192.168.13.20 Pf]]></descr>
3053      <associated-rule-id>nat_57c0187fd4a074.12397754</associated-rule-
3054 id>
```

```
3055      <created>
3056          <time>1472206975</time>
3057          <username>admin@10.97.67.135</username>
3058      </created>
3059      <updated>
3060          <time>1477940348</time>
3061          <username>admin@192.168.13.139</username>
3062      </updated>
3063  </rule>
3064  <rule>
3065      <source>
3066          <any/>
3067      </source>
3068      <destination>
3069          <address>10.33.50.42</address>
3070          <port>2006</port>
3071      </destination>
3072      <protocol>tcp/udp</protocol>
3073      <target>192.168.20.6</target>
3074      <local-port>443</local-port>
3075      <interface>wan</interface>
3076      <descr><! [CDATA[Port Forward to Hytrust Cloud Control
3077 192.168.20.6]]></descr>
3078      <associated-rule-id>nat_585ab274d8bce0.68941358</associated-rule-
3079 id>
3080      <updated>
3081          <time>1482338932</time>
3082          <username>admin@10.97.67.139</username>
3083      </updated>
3084      <created>
3085          <time>1482338932</time>
3086          <username>admin@10.97.67.139</username>
3087      </created>
3088  </rule>
3089  <separator/>
```

```
3090      </nat>
3091      <filter>
3092          <rule>
3093              <id/>
3094              <tracker>1483547179</tracker>
3095              <type>pass</type>
3096              <interface>enc0</interface>
3097              <ipprotocol>inet</ipprotocol>
3098              <tag/>
3099              <tagged/>
3100              <direction>any</direction>
3101              <quick>yes</quick>
3102              <floating>yes</floating>
3103              <max/>
3104              <max-src-nodes/>
3105              <max-src-conn/>
3106              <max-src-states/>
3107              <statetimeout/>
3108              <statetype>keep state</statetype>
3109              <os/>
3110              <source>
3111                  <any/>
3112              </source>
3113              <destination>
3114                  <any/>
3115              </destination>
3116              <descr><! [CDATA[Allow IPSEC Traffic in both directions to
3117      pass]]></descr>
3118              <updated>
3119                  <time>1483547179</time>
3120                  <username>admin@10.97.67.165</username>
3121              </updated>
3122              <created>
3123                  <time>1483547179</time>
```

```
3124             <username>admin@10.97.67.165</username>
3125         </created>
3126     </rule>
3127     <rule>
3128         <id/>
3129         <tracker>1481038469</tracker>
3130         <type>pass</type>
3131         <interface>lan</interface>
3132         <ipprotocol>inet</ipprotocol>
3133         <tag/>
3134         <tagged/>
3135         <direction>any</direction>
3136         <quick>yes</quick>
3137         <floating>yes</floating>
3138         <max/>
3139         <max-src-nodes/>
3140         <max-src-conn/>
3141         <max-src-states/>
3142         <statetimeout/>
3143         <statetype>keep state</statetype>
3144         <os/>
3145         <source>
3146             <address>192.168.14.111</address>
3147         </source>
3148         <destination>
3149             <any/>
3150         </destination>
3151         <descr><! [CDATA[Allow Radiant (192.168.14.111) to go anywhere -
3152 LAN] ]></descr>
3153         <updated>
3154             <time>1481038469</time>
3155             <username>admin@10.97.67.155</username>
3156         </updated>
3157         <created>
```

```
3158          <time>1481038469</time>
3159          <username>admin@10.97.67.155</username>
3160        </created>
3161      </rule>
3162    <rule>
3163      <id/>
3164      <tracker>1481134883</tracker>
3165      <type>pass</type>
3166      <interface>lan</interface>
3167      <ipprotocol>inet</ipprotocol>
3168      <tag/>
3169      <tagged/>
3170      <direction>any</direction>
3171      <quick>yes</quick>
3172      <floating>yes</floating>
3173      <max/>
3174      <max-src-nodes/>
3175      <max-src-conn/>
3176      <max-src-states/>
3177      <statetimeout/>
3178      <statetype>keep state</statetype>
3179      <os/>
3180      <source>
3181        <address>192.168.13.135</address>
3182      </source>
3183      <destination>
3184        <any/>
3185      </destination>
3186      <descr><! [CDATA[Allow CA.acmefinancial to go anywhere]]></descr>
3187      <updated>
3188        <time>1481134883</time>
3189        <username>admin@10.97.67.146</username>
3190      </updated>
3191      <created>
```

```
3192          <time>1481134883</time>
3193          <username>admin@10.97.67.146</username>
3194        </created>
3195      </rule>
3196    <rule>
3197      <id/>
3198      <tracker>1481038517</tracker>
3199      <type>pass</type>
3200      <interface>lan</interface>
3201      <ipprotocol>inet</ipprotocol>
3202      <tag/>
3203      <tagged/>
3204      <direction>any</direction>
3205      <quick>yes</quick>
3206      <floating>yes</floating>
3207      <max/>
3208      <max-src-nodes/>
3209      <max-src-conn/>
3210      <max-src-states/>
3211      <statetimeout/>
3212      <statetype>keep state</statetype>
3213      <os/>
3214    <source>
3215      <address>192.168.17.100</address>
3216    </source>
3217    <destination>
3218      <any/>
3219    </destination>
3220    <descr><![CDATA[Allow Radiant (192.168.17.100) to go anywhere -
3221 LAN]]></descr>
3222    <updated>
3223      <time>1481038517</time>
3224      <username>admin@10.97.67.155</username>
3225    </updated>
```

```
3226          <created>
3227              <time>1481038517</time>
3228              <username>admin@10.97.67.155</username>
3229          </created>
3230      </rule>
3231      <rule>
3232          <id/>
3233          <tracker>1478010422</tracker>
3234          <type>pass</type>
3235          <interface>wan</interface>
3236          <ipprotocol>inet</ipprotocol>
3237          <tag/>
3238          <tagged/>
3239          <direction>any</direction>
3240          <quick>yes</quick>
3241          <floating>yes</floating>
3242          <max/>
3243          <max-src-nodes/>
3244          <max-src-conn/>
3245          <max-src-states/>
3246          <statetimeout/>
3247          <statetype>keep state</statetype>
3248          <os/>
3249          <source>
3250              <any/>
3251          </source>
3252          <destination>
3253              <any/>
3254          </destination>
3255          <descr/>
3256          <updated>
3257              <time>1478010422</time>
3258              <username>admin@10.97.66.18</username>
3259          </updated>
```

```
3260          <created>
3261              <time>1478010422</time>
3262              <username>admin@10.97.66.18</username>
3263          </created>
3264      </rule>
3265      <rule>
3266          <id/>
3267          <tracker>1480540664</tracker>
3268          <type>pass</type>
3269          <interface>lan</interface>
3270          <ipprotocol>inet</ipprotocol>
3271          <tag/>
3272          <tagged/>
3273          <direction>any</direction>
3274          <quick>yes</quick>
3275          <floating>yes</floating>
3276          <max/>
3277          <max-src-nodes/>
3278          <max-src-conn/>
3279          <max-src-states/>
3280          <statetimeout/>
3281          <statetype>keep state</statetype>
3282          <os/>
3283          <source>
3284              <any/>
3285          </source>
3286          <destination>
3287              <any/>
3288          </destination>
3289          <descr><! [CDATA[Allow all LAN traffic to go to anywhere]]></descr>
3290          <updated>
3291              <time>1480540664</time>
3292              <username>admin@10.97.67.140</username>
3293          </updated>
```

```
3294             <created>
3295                 <time>1480540664</time>
3296                 <username>admin@10.97.67.140</username>
3297             </created>
3298         </rule>
3299     <rule>
3300         <id/>
3301         <tracker>1472208251</tracker>
3302         <type>pass</type>
3303         <interface>lan</interface>
3304         <ipprotocol>inet</ipprotocol>
3305         <tag/>
3306         <tagged/>
3307         <direction>any</direction>
3308         <quick>yes</quick>
3309         <floating>yes</floating>
3310         <max/>
3311         <max-src-nodes/>
3312         <max-src-conn/>
3313         <max-src-states/>
3314         <statetimeout/>
3315         <statetype>keep state</statetype>
3316         <os/>
3317         <protocol>tcp/udp</protocol>
3318         <source>
3319             <address>192.168.0.0/16</address>
3320         </source>
3321         <destination>
3322             <address>192.168.0.0/16</address>
3323         </destination>
3324         <descr><! [CDATA[Allow traffic going from local subnet to local
3325 subne] ]></descr>
3326         <updated>
3327             <time>1472208251</time>
```

```
3328                  <username>admin@10.97.67.135</username>
3329                  </updated>
3330                  <created>
3331                      <time>1472208251</time>
3332                      <username>admin@10.97.67.135</username>
3333                  </created>
3334              </rule>
3335          <rule>
3336              <id/>
3337              <tracker>1472216936</tracker>
3338              <type>pass</type>
3339              <interface>lan</interface>
3340              <ipprotocol>inet</ipprotocol>
3341              <tag/>
3342              <tagged/>
3343              <direction>any</direction>
3344              <quick>yes</quick>
3345              <floating>yes</floating>
3346              <max/>
3347              <max-src-nodes/>
3348              <max-src-conn/>
3349              <max-src-states/>
3350              <statetimeout/>
3351              <statetype>keep state</statetype>
3352              <os/>
3353              <protocol>tcp/udp</protocol>
3354          <source>
3355              <address>192.168.0.0/16</address>
3356          </source>
3357          <destination>
3358              <any/>
3359          </destination>
3360          <descr><! [CDATA[Allow traffic going from local subnet to
3361 anywhere]]></descr>
```

```
3362      <updated>
3363          <time>1472216936</time>
3364          <username>admin@10.97.67.135</username>
3365      </updated>
3366      <created>
3367          <time>1472216936</time>
3368          <username>admin@10.97.67.135</username>
3369      </created>
3370  </rule>
3371  <rule>
3372      <id/>
3373      <tracker>1476720725</tracker>
3374      <type>pass</type>
3375      <interface>enc0</interface>
3376      <ipprotocol>inet</ipprotocol>
3377      <tag/>
3378      <tagged/>
3379      <direction>any</direction>
3380      <quick>yes</quick>
3381      <floating>yes</floating>
3382      <max/>
3383      <max-src-nodes/>
3384      <max-src-conn/>
3385      <max-src-states/>
3386      <statetimeout/>
3387      <statetype>keep state</statetype>
3388      <os/>
3389      <source>
3390          <any/>
3391      </source>
3392      <destination>
3393          <any/>
3394      </destination>
```

```
3395      <descr><! [CDATA[Allow All traffic sourced from Tunnel to Anywhere  
3396 o]></descr>  
3397      <updated>  
3398          <time>1476720725</time>  
3399          <username>admin@10.97.67.137</username>  
3400      </updated>  
3401      <created>  
3402          <time>1476720725</time>  
3403          <username>admin@10.97.67.137</username>  
3404      </created>  
3405      </rule>  
3406      <rule>  
3407          <id/>  
3408          <tracker>1471551236</tracker>  
3409          <type>pass</type>  
3410          <interface>wan</interface>  
3411          <ipprotocol>inet</ipprotocol>  
3412          <tag/>  
3413          <tagged/>  
3414          <max/>  
3415          <max-src-nodes/>  
3416          <max-src-conn/>  
3417          <max-src-states/>  
3418          <statetimeout/>  
3419          <statetype>keep state</statetype>  
3420          <os/>  
3421          <protocol>tcp/udp</protocol>  
3422          <source>  
3423              <any/>  
3424          </source>  
3425          <destination>  
3426              <any/>  
3427          </destination>  
3428      <descr><! [CDATA[Allow all TCP/UDP Traffic sourced from WAN  
3429 interface]]></descr>
```

```
3430          <updated>
3431              <time>1471551236</time>
3432              <username>admin@10.97.67.136</username>
3433          </updated>
3434          <created>
3435              <time>1471551236</time>
3436              <username>admin@10.97.67.136</username>
3437          </created>
3438      </rule>
3439      <rule>
3440          <id/>
3441          <tracker>1470759134</tracker>
3442          <type>pass</type>
3443          <interface>wan</interface>
3444          <ipprotocol>inet</ipprotocol>
3445          <tag/>
3446          <tagged/>
3447          <max/>
3448          <max-src-nodes/>
3449          <max-src-conn/>
3450          <max-src-states/>
3451          <statetimeout/>
3452          <statetype>keep state</statetype>
3453          <os/>
3454          <protocol>tcp/udp</protocol>
3455          <source>
3456              <any/>
3457          </source>
3458          <destination>
3459              <network>(self)</network>
3460          </destination>
3461          <descr><! [CDATA[Rule to allow connection to firewall -can be
3462 tighten]]></descr>
3463          <updated>
```

```
3464          <time>1470759134</time>
3465          <username>admin@192.168.13.135</username>
3466        </updated>
3467        <created>
3468          <time>1470759134</time>
3469          <username>admin@192.168.13.135</username>
3470        </created>
3471      </rule>
3472      <rule>
3473        <id/>
3474        <tracker>1461788221</tracker>
3475        <type>pass</type>
3476        <interface>wan</interface>
3477        <ipprotocol>inet</ipprotocol>
3478        <tag/>
3479        <tagged/>
3480        <max/>
3481        <max-src-nodes/>
3482        <max-src-conn/>
3483        <max-src-states/>
3484        <statetimeout/>
3485        <statetype>keep state</statetype>
3486        <os/>
3487        <protocol>tcp</protocol>
3488        <source>
3489          <any/>
3490        </source>
3491        <destination>
3492          <any/>
3493        </destination>
3494        <descr/>
3495        <updated>
3496          <time>1461788221</time>
3497          <username>admin@192.168.1.2</username>
```

```
3498          </updated>
3499          <created>
3500              <time>1461788221</time>
3501              <username>admin@192.168.1.2</username>
3502          </created>
3503      </rule>
3504      <rule>
3505          <id/>
3506          <tracker>1465934823</tracker>
3507          <type>pass</type>
3508          <interface>wan</interface>
3509          <ipprotocol>inet</ipprotocol>
3510          <tag/>
3511          <tagged/>
3512          <max/>
3513          <max-src-nodes/>
3514          <max-src-conn/>
3515          <max-src-states/>
3516          <statetimeout/>
3517          <statetype>keep state</statetype>
3518          <os/>
3519          <protocol>icmp</protocol>
3520          <source>
3521              <any/>
3522          </source>
3523          <destination>
3524              <any/>
3525          </destination>
3526          <descr><![CDATA[Easy Rule: Passed from Firewall Log
3527 View]]></descr>
3528          <created>
3529              <time>1465934786</time>
3530              <username>Easy Rule</username>
3531          </created>
```

```
3532             <updated>
3533                 <time>1465934839</time>
3534                 <username>admin@192.168.13.101</username>
3535             </updated>
3536         </rule>
3537     <rule>
3538         <source>
3539             <any/>
3540         </source>
3541         <interface>wan</interface>
3542         <protocol>tcp/udp</protocol>
3543         <destination>
3544             <address>192.168.19.11</address>
3545             <port>80</port>
3546         </destination>
3547         <descr><![CDATA[NAT Port forward to openldap; Add /phpldapadmin to
3548 address]]></descr>
3549         <associated-rule-id>nat_57bf0c96d083f4.07194849</associated-rule-
3550 id>
3551         <tracker>1472138390</tracker>
3552         <created>
3553             <time>1472138390</time>
3554             <username>NAT Port Forward</username>
3555         </created>
3556     </rule>
3557     <rule>
3558         <source>
3559             <any/>
3560         </source>
3561         <interface>wan</interface>
3562         <protocol>tcp/udp</protocol>
3563         <destination>
3564             <address>192.168.13.14</address>
3565             <port>80</port>
3566         </destination>
```

```
3567          <descr><! [CDATA[NAT Port Forward to 192.168.13.14 Pf] ]></descr>
3568          <associated-rule-id>nat_57c01545c247f0.43308393</associated-rule-
3569      id>
3570          <tracker>1472206149</tracker>
3571          <created>
3572              <time>1472206149</time>
3573              <username>NAT Port Forward</username>
3574          </created>
3575      </rule>
3576      <rule>
3577          <source>
3578              <any/>
3579          </source>
3580          <interface>wan</interface>
3581          <protocol>tcp/udp</protocol>
3582          <destination>
3583              <address>192.168.13.15</address>
3584              <port>80</port>
3585          </destination>
3586          <descr><! [CDATA[NAT Port Forward to 192.168.13.15 Pf] ]></descr>
3587          <associated-rule-id>nat_57c0163d6e2de9.62906352</associated-rule-
3588      id>
3589          <tracker>1472206397</tracker>
3590          <created>
3591              <time>1472206397</time>
3592              <username>NAT Port Forward</username>
3593          </created>
3594      </rule>
3595      <rule>
3596          <source>
3597              <any/>
3598          </source>
3599          <interface>wan</interface>
3600          <protocol>tcp/udp</protocol>
3601          <destination>
```

```
3602             <address>192.168.13.16</address>
3603                 <port>80</port>
3604             </destination>
3605             <descr><! [CDATA[NAT Port Forward to 192.168.13.16 Pf] ]></descr>
3606             <associated-rule-id>nat_57c01682da98c4.72334719</associated-rule-
3607 id>
3608             <tracker>1472206466</tracker>
3609             <created>
3610                 <time>1472206466</time>
3611                 <username>NAT Port Forward</username>
3612             </created>
3613         </rule>
3614         <rule>
3615             <source>
3616                 <any/>
3617             </source>
3618             <interface>wan</interface>
3619             <protocol>tcp/udp</protocol>
3620             <destination>
3621                 <address>192.168.13.17</address>
3622                 <port>80</port>
3623             </destination>
3624             <descr><! [CDATA[NAT Port Forward to 192.168.13.17 Pf] ]></descr>
3625             <associated-rule-id>nat_57c01787b4e891.75909166</associated-rule-
3626 id>
3627             <tracker>1472206727</tracker>
3628             <created>
3629                 <time>1472206727</time>
3630                 <username>NAT Port Forward</username>
3631             </created>
3632         </rule>
3633         <rule>
3634             <source>
3635                 <any/>
3636             </source>
```

```
3637             <interface>wan</interface>
3638             <protocol>tcp/udp</protocol>
3639             <destination>
3640                 <address>192.168.13.18</address>
3641                 <port>80</port>
3642             </destination>
3643             <descr><! [CDATA[NAT Port Forward to 192.168.13.18 Pf] ]></descr>
3644             <associated-rule-id>nat_57c017be3dfffa1.16882401</associated-rule-
3645 id>
3646             <tracker>1472206782</tracker>
3647             <created>
3648                 <time>1472206782</time>
3649                 <username>NAT Port Forward</username>
3650             </created>
3651         </rule>
3652         <rule>
3653             <source>
3654                 <any/>
3655             </source>
3656             <interface>wan</interface>
3657             <protocol>tcp/udp</protocol>
3658             <destination>
3659                 <address>192.168.13.19</address>
3660                 <port>80</port>
3661             </destination>
3662             <descr><! [CDATA[NAT Port Forward to 192.168.13.19 Pf] ]></descr>
3663             <associated-rule-id>nat_57c017e1e48d65.86612217</associated-rule-
3664 id>
3665             <tracker>1472206817</tracker>
3666             <created>
3667                 <time>1472206817</time>
3668                 <username>NAT Port Forward</username>
3669             </created>
3670         </rule>
3671         <rule>
```

```
3672             <source>
3673                 <any/>
3674             </source>
3675             <interface>wan</interface>
3676             <protocol>tcp/udp</protocol>
3677             <destination>
3678                 <address>192.168.13.20</address>
3679                 <port>80</port>
3680             </destination>
3681             <descr><! [CDATA[NAT Port Forward to 192.168.13.20 Pf] ]></descr>
3682             <associated-rule-id>nat_57c0187fd4a074.12397754</associated-rule-
3683 id>
3684             <tracker>1472206975</tracker>
3685             <created>
3686                 <time>1472206975</time>
3687                 <username>NAT Port Forward</username>
3688             </created>
3689         </rule>
3690         <rule>
3691             <source>
3692                 <any/>
3693             </source>
3694             <interface>wan</interface>
3695             <protocol>tcp/udp</protocol>
3696             <destination>
3697                 <address>192.168.17.10</address>
3698                 <port>8000</port>
3699             </destination>
3700             <descr><! [CDATA[NAT Splunk port 8000 Web Interface] ]></descr>
3701             <associated-rule-id>nat_57d825ba865df6.65796295</associated-rule-
3702 id>
3703             <tracker>1473783226</tracker>
3704             <created>
3705                 <time>1473783226</time>
3706                 <username>NAT Port Forward</username>
```

```
3707                  </created>
3708          </rule>
3709      <rule>
3710          <source>
3711              <any/>
3712          </source>
3713          <interface>wan</interface>
3714          <protocol>tcp/udp</protocol>
3715          <destination>
3716              <address>192.168.19.11</address>
3717              <port>22</port>
3718          </destination>
3719          <descr><! [CDATA[NAT Port forward to openldap; ]]></descr>
3720          <associated-rule-id>nat_57f555406f2de3.01889708</associated-rule-
3721 id>
3722          <tracker>1475695936</tracker>
3723          <created>
3724              <time>1475695936</time>
3725              <username>NAT Port Forward</username>
3726          </created>
3727      </rule>
3728      <rule>
3729          <source>
3730              <any/>
3731          </source>
3732          <interface>wan</interface>
3733          <protocol>tcp</protocol>
3734          <destination>
3735              <address>192.168.13.130</address>
3736              <port>80</port>
3737          </destination>
3738          <descr><! [CDATA[NAT Mapping to pfsense 192.168.13.130]]></descr>
3739          <associated-rule-id>nat_581795efbc2944.51341500</associated-rule-
3740 id>
3741          <tracker>1477940719</tracker>
```

```
3742             <created>
3743                 <time>1477940719</time>
3744                 <username>NAT Port Forward</username>
3745             </created>
3746         </rule>
3747     <rule>
3748         <source>
3749             <any/>
3750         </source>
3751         <interface>wan</interface>
3752         <protocol>tcp/udp</protocol>
3753         <destination>
3754             <address>192.168.17.10</address>
3755             <port>22</port>
3756         </destination>
3757         <descr><! [CDATA[NAT Splunk SSH ]]></descr>
3758         <associated-rule-id>nat_582ef78ed63d23.63868026</associated-rule-
3759     id>
3760         <tracker>1479473038</tracker>
3761         <created>
3762             <time>1479473038</time>
3763             <username>NAT Port Forward</username>
3764         </created>
3765     </rule>
3766     <rule>
3767         <source>
3768             <any/>
3769         </source>
3770         <interface>wan</interface>
3771         <protocol>tcp/udp</protocol>
3772         <destination>
3773             <address>192.168.20.6</address>
3774             <port>443</port>
3775         </destination>
```

```
3776      <descr><![CDATA[NAT Port Forward to Hytrust Cloud Control  
3777 192.168.20.6]]></descr>  
3778      <associated-rule-id>nat_585ab274d8bce0.68941358</associated-rule-  
3779 id>  
3780      <tracker>1482338932</tracker>  
3781      <created>  
3782          <time>1482338932</time>  
3783          <username>NAT Port Forward</username>  
3784      </created>  
3785      </rule>  
3786      <rule>  
3787          <id/>  
3788          <tracker>1480540738</tracker>  
3789          <type>pass</type>  
3790          <interface>lan</interface>  
3791          <ipprotocol>inet</ipprotocol>  
3792          <tag/>  
3793          <tagged/>  
3794          <max/>  
3795          <max-src-nodes/>  
3796          <max-src-conn/>  
3797          <max-src-states/>  
3798          <statetimeout/>  
3799          <statetype>keep state</statetype>  
3800          <os/>  
3801          <source>  
3802              <any/>  
3803          </source>  
3804          <destination>  
3805              <any/>  
3806          </destination>  
3807          <descr><![CDATA[Allow all LAN traffic to go to anywhere]]></descr>  
3808          <updated>  
3809              <time>1480540738</time>  
3810              <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>
```

```
3879          <interface>enc0</interface>
3880          <ipprotocol>inet</ipprotocol>
3881          <tag/>
3882          <tagged/>
3883          <max/>
3884          <max-src-nodes/>
3885          <max-src-conn/>
3886          <max-src-states/>
3887          <statetimeout/>
3888          <statetype>keep state</statetype>
3889          <os/>
3890          <source>
3891              <any/>
3892          </source>
3893          <destination>
3894              <any/>
3895          </destination>
3896          <descr><! [CDATA[Allow All traffic sourced from Tunnel to Anywhere
3897 o]]></descr>
3898          <created>
3899              <time>1476720530</time>
3900              <username>admin@10.97.67.137</username>
3901          </created>
3902          <updated>
3903              <time>1476720628</time>
3904              <username>admin@10.97.67.137</username>
3905          </updated>
3906      </rule>
3907      <separator>
3908          <lan/>
3909          <wan/>
3910          <floatingrules/>
3911          <enc0/>
3912      </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>
```

```
3947      <client/>
3948      <phase2>
3949          <ikeid>1</ikeid>
3950          <unqid>5804f45c4f196</unqid>
3951          <mode>tunnel</mode>
3952          <reqid>1</reqid>
3953          <localid>
3954              <type>network</type>
3955              <address>192.168.19.0</address>
3956              <netbits>24</netbits>
3957          </localid>
3958          <remoteid>
3959              <type>network</type>
3960              <address>172.17.212.0</address>
3961              <netbits>24</netbits>
3962          </remoteid>
3963          <protocol>esp</protocol>
3964          <encryption-algorithm-option>
3965              <name>aes</name>
3966              <keylen>256</keylen>
3967          </encryption-algorithm-option>
3968          <hash-algorithm-option>hmac_shal</hash-algorithm-option>
3969          <pfsgroup>0</pfsgroup>
3970          <lifetime>3600</lifetime>
3971          <pinghost/>
3972          <descr><! [CDATA[Phase 2 IPSEC Tunnel to Vanguard] ]></descr>
3973      </phase2>
3974      <phase2>
3975          <ikeid>1</ikeid>
3976          <unqid>586d5ecf7f516</unqid>
3977          <mode>tunnel</mode>
3978          <reqid>2</reqid>
3979          <localid>
3980              <type>network</type>
```

```
3981             <address>192.168.17.0</address>
3982                 <netbits>24</netbits>
3983             </localid>
3984             <remoteid>
3985                 <type>network</type>
3986                     <address>172.17.212.0</address>
3987                     <netbits>24</netbits>
3988             </remoteid>
3989             <protocol>esp</protocol>
3990             <encryption-algorithm-option>
3991                 <name>aes</name>
3992                 <keylen>256</keylen>
3993             </encryption-algorithm-option>
3994             <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
3995             <pfsgroup>0</pfsgroup>
3996             <lifetime>3600</lifetime>
3997             <pinghost/>
3998             <descr><! [CDATA[Phase 2 IPSEC Tunnel to Vanguard] ]></descr>
3999         </phase2>
4000         <phase2>
4001             <ikeid>1</ikeid>
4002             <unqid>586d5eeb02957</unqid>
4003             <mode>tunnel</mode>
4004             <reqid>3</reqid>
4005             <localid>
4006                 <type>network</type>
4007                     <address>192.168.13.0</address>
4008                     <netbits>24</netbits>
4009             </localid>
4010             <remoteid>
4011                 <type>network</type>
4012                     <address>172.17.212.0</address>
4013                     <netbits>24</netbits>
4014             </remoteid>
```

```
4015      <protocol>esp</protocol>
4016      <encryption-algorithm-option>
4017          <name>aes</name>
4018          <keylen>256</keylen>
4019      </encryption-algorithm-option>
4020      <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
4021      <pfsgroup>0</pfsgroup>
4022      <lifetime>3600</lifetime>
4023      <pinghost/>
4024      <descr><! [CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
4025  </phase2>
4026  <phase2>
4027      <ikeid>1</ikeid>
4028      <unqid>586d5f54943b4</unqid>
4029      <mode>tunnel</mode>
4030      <reqid>4</reqid>
4031      <localid>
4032          <type>network</type>
4033          <address>192.168.14.0</address>
4034          <netbits>24</netbits>
4035      </localid>
4036      <remoteid>
4037          <type>network</type>
4038          <address>172.17.212.0</address>
4039          <netbits>24</netbits>
4040      </remoteid>
4041      <protocol>esp</protocol>
4042      <encryption-algorithm-option>
4043          <name>aes</name>
4044          <keylen>256</keylen>
4045      </encryption-algorithm-option>
4046      <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
4047      <pfsgroup>0</pfsgroup>
4048      <lifetime>3600</lifetime>
```

```
4049          <pinghost/>
4050          <descr><! [CDATA[Phase 2 IPSEC Tunnel to Vanguard] ]></descr>
4051      </phase2>
4052      </ipsec>
4053      <aliases/>
4054      <proxyarp/>
4055      <cron>
4056          <item>
4057              <minute>1,31</minute>
4058              <hour>0-5</hour>
4059              <mday>*</mday>
4060              <month>*</month>
4061              <wday>*</wday>
4062              <who>root</who>
4063              <command>/usr/bin/nice -n20 adjkerntz -a</command>
4064          </item>
4065          <item>
4066              <minute>1</minute>
4067              <hour>3</hour>
4068              <mday>1</mday>
4069              <month>*</month>
4070              <wday>*</wday>
4071              <who>root</who>
4072              <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
4073          </item>
4074          <item>
4075              <minute>*/60</minute>
4076              <hour>*</hour>
4077              <mday>*</mday>
4078              <month>*</month>
4079              <wday>*</wday>
4080              <who>root</who>
4081              <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4082      sshlockout</command>
```

```
4083          </item>
4084
4085          <item>
4086              <minute>*/60</minute>
4087              <hour>*</hour>
4088              <mday>*</mday>
4089              <month>*</month>
4090              <wday>*</wday>
4091              <who>root</who>
4092          <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4092      webConfiguratorlockout</command>
4093
4094          </item>
4095
4096          <item>
4097              <minute>1</minute>
4098              <hour>1</hour>
4099              <mday>*</mday>
4100              <month>*</month>
4101              <wday>*</wday>
4102              <who>root</who>
4103          <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
4104
4105          </item>
4106
4107          <item>
4108              <minute>*/60</minute>
4109              <hour>*</hour>
4110              <mday>*</mday>
4111              <month>*</month>
4112              <wday>*</wday>
4113              <who>root</who>
4114          <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4114      virusprot</command>
4115
4116          </item>
4117
4118          <item>
4119              <minute>30</minute>
4120              <hour>12</hour>
4121              <mday>*</mday>
4122              <month>*</month>
```

```
4118          <wday>*</wday>
4119          <who>root</who>
4120          <command>/usr/bin/nice -n20 /etc/rc.update_urllables</command>
4121      </item>
4122  </cron>
4123  <wol/>
4124  <rrd>
4125      <enable/>
4126  </rrd>
4127  <load_balancer>
4128      <monitor_type>
4129          <name>ICMP</name>
4130          <type>icmp</type>
4131          <descr><! [CDATA[ ICMP ]></descr>
4132          <options/>
4133      </monitor_type>
4134      <monitor_type>
4135          <name>TCP</name>
4136          <type>tcp</type>
4137          <descr><! [CDATA[ Generic TCP ]></descr>
4138          <options/>
4139      </monitor_type>
4140      <monitor_type>
4141          <name>HTTP</name>
4142          <type>http</type>
4143          <descr><! [CDATA[ Generic HTTP ]></descr>
4144          <options>
4145              <path>/</path>
4146              <host/>
4147              <code>200</code>
4148          </options>
4149      </monitor_type>
4150      <monitor_type>
4151          <name>HTTPS</name>
```

```
4152      <type>https</type>
4153      <descr><! [CDATA[Generic HTTPS] ]></descr>
4154      <options>
4155          <path>/</path>
4156          <host/>
4157          <code>200</code>
4158      </options>
4159  </monitor_type>
4160  <monitor_type>
4161      <name>SMTP</name>
4162      <type>send</type>
4163      <descr><! [CDATA[Generic SMTP] ]></descr>
4164      <options>
4165          <send/>
4166          <expect>220 *</expect>
4167      </options>
4168  </monitor_type>
4169  </load_balancer>
4170  <widgets>
4171      <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
4172 /sequence>
4173      </widgets>
4174      <openvpn/>
4175      <dnshaper/>
4176      <unbound>
4177          <enable/>
4178          <dnssec/>
4179          <active_interface/>
4180          <outgoing_interface/>
4181          <custom_options/>
4182          <hideidentity/>
4183          <hideversion/>
4184          <dnssecstripped/>
4185      </unbound>
```

```

4187      <dhcpdv6>
4188          </lan>
4189          <range>
4190              <from>::1000</from>
4191              <to>::2000</to>
4192          </range>
4193          <ramode>assist</ramode>
4194          <rapriority>medium</rapriority>
4195      </lan>
4196  </dhcpdv6>
4197  <cert>
4198      <refid>5720a0502b277</refid>
4199      <descr><![CDATA[webConfigurator default (5720a0502b277) ]]></descr>
4200      <type>server</type>
4201      <crt>LS0tLS1CRUDJTibDRVJUSUZJQ0FURS0tLS0tCk1JSUziVENDQkZXZ0F3SUJBZ01CQURBTkJna3
4202 Foa21HOXcwQkFRc0ZBRENcdERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnT1ZCQWdUQ1ZOMF1YUmxBNUkV3RHdZ
4203 RFZRUUhFd2hNYjJoaGJhbDB1VEU0TURZR0ExVUVDaE12Y0daVApaVzV6W1NCM1pXSkrMiMjVtYVdkMWNTRjBiM0
4204 lnVTJWc1ppMVRhV2R1W1dRZ1EyVn1kR2xtYVdOaGRHVxhLREFtCkJna3Foa21HOXcwQkNRRVdHV0ZrY1dsdVFI
4205 Qm1VMlZ1YzJvDwJHOpwZV3hrYjIxaGFVNHHIakFjQmdOVkJBTvQKRlhCbVUyVnVjM1V0T1RjeU1HRXdOVEF5WW
4206 pJM056QWVGdzB4TmpBME1qY3hNEU1TkRSYUZ3MH1NVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
4207 d0pWVxpFT01Bd0dBMVVFQ0JNR1UzUmhkR1V4RVRBUEJnT1ZCQWNNUCKNFehZZMkZzYVhSNU1Uz3dOZ11EV1FRS0
4208 V5OXdabE5sYm5ObE1IZGxza052Ym1acFo2Vn1ZWFJ2Y21CVFpXeG0KTFZoCfOyNWxaQ0JEWlhKMGFxWnBZMkYw
4209 W1Rfb01DWUDDU3FHU01iM0RRRUpBU1laWVdSdGFXNUFjR1pUW1clegpaUzVzYjJoaGJHUnZiV0ZwYmpFZU1Cd0
4210 dBMVVFQXhNVmNHw1RaVzV6W1MwMU56SXdZVEExTURKaU1qYzNNSU1CCk1qU5CZ2txaGtpRz13MEJBuuVGQUFP
4211 Q0FROEFNSU1CQ2dLQ0FRRUF0L085aD1nT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NwCgJNYXFmUE1aVzNMdG
4212 hDODBH0dhZnJENwdqctrwZkNNMH1zbEFPaV1ZK1hDYjdnA200dmtTMgpmbz14emNyadUrNV1aY1BHeXR1a21s
4213 ZWR4bjFWef16S11zYXZKdn1Kb11RMctNTkx0dkFjYnRhTUfOzjh1ZkRFC1hrc1NVQ0N5YTFrbEYxNWJGZmcyUG
4214 E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkuFRJTkx3QUZnd1E5K1BQZkwKVTQxFMBVb3FFbWEwdzU4Q1RZKzZh
4215 ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxDmdCUApyeXd1SEZwd3J1LytyWExieEcrcD
4216 dwYXI0aHR0UFRDcm11NmFqQVVTNmpvN05kOE1QNWPzZ1kzR0h2ZjhZUU1ECKfRQUJvNE1CaGpDQ0FZSXdDUV1E
4217 V1IwVEJBSxdBREFSQmdsZ2hrZ0JodmhDQVFFRJBTUNCa0F3TxdZs11JWkkQV1iNFFnRu5CQ11XskU5d1pXNV
4218 RVIMHdnUjJwdVpYSmhkr1ZrSUZobGNuWmxjaUJEWlhKMGFxWnBZMkYwW1RBZApCZ05WSFE0RUznuVU3K11LrmNp
4219 OFFVSGhTZ0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K11LckZjaThRVuhoU2dMRHY4RUNzY0
4220 NKd0FLaGdicWtnYmN3Z2JReEN6QuPCZ05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
4221 VUVCeE1JVec5allXeHBkSGt4T0RBMkJnT1ZCQW9UTDNCbVuYVnVjM1VnZDJWaQpRmj11Wm1sbmRYSmhkRz15SU
4222 ZOBGJHWXRVMmxuYm1Wa01FTmxjb1JwWm1sa11YUmxBu2d3SmdZsktvWk1odmNOCKfRa0JGaGx0WkcxcGJrQnda
4223 bE5sYm5ObExteHZZMkzzWkc5dF1XbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
4224 56ZUNBUUF3SFFZRFZSMGxCQ113RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd01G
4225 b0RBTkJna3Foa21HOXcwQkFRc0ZBQU9DQVFFQXjxFpQdXd2MVzuUC82NmJDWFJ5CkVmaW1LRw1PcmtNaTB5M0
4226 9PWGtzWEs1cEM2dTd6Uk13WjEvRjYyRUp3OD1UOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWjhRu42NEkxOHFud3Zm
4227 S2JrREZvRThMR1hSdzBkMnAyTGVmYTd4YTIVsGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTs9wV3p3aDdQRG
4228 c4bGdrcVc3dSt1b01DNDJ1bVjkOURCTmlzdFJ4Rv1NmKfLQkFsZG1LYStvRUY1VUuwCm43aXpvN1Z4dHJWMTJv
4229 TTdyS11RQ05kY00xZkvSeUwvb3ZkUnVpa0F5Wm1VvnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOvpPSmR2QmZLVU
4230 1sUW1ELyswSVpTa1FXRDczWkdlsaEhTK2t0eWc1aDjhUjUwYjh3Wm9zQnNjSUZDa0pFbgp0UT09Ci0tLS0tRU5E
4231 IENF1lRJRk1DQVRFLS0tLS0K</crt>
4232
4233 <prv>LS0tLS1CRUDJTibBQuk1WQVRFIetFWS0tLS0tCk1JSUV2Z01CQURBTkJna3Foa21HOXcwQkFRRU
4234 ZBQVNDQktn2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M01hY1kKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4
4235

```

```

4236 eGxiY3UyRUX6UVpJWnArc1BtQ09yaWw4SXpUS31VQTZKaGo1YwpKdnN5U1BpK1JMWithqM0hOeXVIbjdsagxzOG
4237 JLMjZTS1Y1M0dmV1hGak1saXhxOG0vSW1oaERUNHcwtI4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEpyV1NVWFhs
4238 c1YrRFk5cmpGMmpZNDrSE1iU1JZSWxLUHo1TzVtNTA5TWcwkEKQVdEQkQzNDg5OHRUalhROVNpb1NaclREbn
4239 dKTmo3cHAwQnM4ZH1RDBjL2poUGFWswNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
4240 dHZFYjZudWxxdm1HMja5TUT1Szdwcu1CUkxxT2pzMTN3Zy9tT31CCmpjWWU5L314QWdNQkfBRUNnz0VCQUpRRF
4241 pxU3duMnNTUTh0SVNBTVUrUW0zcXhrb3BzdzB4cWNScmFl0Ed4VmQKejBpOU1KbkZVQWFleTQvL3J1dndhzW1P
4242 R3RYSmZ2ai9jSnY3cmJIWGIzYkJtVW9hcDhxY0RjdVSMmlHRUZYWQpCL3hjNVpINTlaTUFabWE1VVWQLzNjcD
4243 1zNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVDk1CjNLrmk4VTZUM1hnU1c2eFowZHp1Zn1P
4244 UzAvbXlmNU5YLzVoRk1PNmFDc0x1UjZ4N1Rza2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
4245 hMZ0NRY1B2MnE5V0Nia0VMNEZUZmRz1ZxcHBRNG1ZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
4246 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUe0NzNMUWoxcExLSmRZN2JxCmtMU3NVT0zHTUZ1ZG1xU2ttbzh3Qj
4247 1pMXhbE1LQUD0M3U4dTdMz1ztU2lybnMwVVBTMHRVUDRyQXmzVFJocEgKU2Z4VXVsbgVGaKtzk9xRE11TTBC
4248 OGttbFJnUFrmVHVPaGNwMGVkmQwK1E5Y2V1Y25kaFp3UE16TUC3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHNhb
4249 NBRDhVYThDZ11FQXpzYjYzbzRBSH1YNjZkcEJ6TG1zYzZxs2d2ZG4xazhVcm02N3RuK2M3NkVhSEtZT1k0Rjdh
4250 S0dFSk1yeU0yQTJTTe1Azdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUpOK013Sm
4251 Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHvtQOpJZm1DW1pRSUQ1OENnWUJjamFO
4252 dk5obnFJOG9rWGHBUjR2c3NtNGpWb0tyU1ZScjRIVHo5MDFwOGdReXNCWkt0Cn1US2V6VThuUVZvTjNYWmVMBc
4253 8rVEcwYVpKOTZHKy9nNTRWZmZqWTR1elVScHhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHNOZuaGI0cUFjNHBWSUc3
4254 QWY5Mi9CbHZJR25FS1pMdnhLWTdvmX1Ib1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdgJNTn
4255 VudmNUUjZxtzR0ekZtdG5TYWN3W1Ftb2UvdUVIaGE0bU84WTBCeTNRcitu1BCCndVR2RiUnNhdTgxcU12VUtu
4256 RG1hZGsvKy9Ud2Uvvk1Kbmxt2W9zS3VjTG42Y1c2eGVhR1hFc3FoUjlhbkwzRjMKcEpUSGg4Y3FsNTdqdKRRN0
4257 FBamdyQmxrb3pOVnNMZThiWWpkcHR1MVBRs0JnQ0xDR0R1RXNBYUxwZ1RtOG44bgoyQ1h1NE52K113a1Rlczdu
4258 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSvdyCnRCZ1ZLC1UzSThhYnpnUUtwOEwrzj
4259 VadTAxY1pZVk5TU0FIURHYm5jb1IzbGVPyjNLeUVXQjdsZFBHQwpOS3UwNkd5TEkKakh5TDhadEFBRXBZ1FU
4260 OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEugS0VZLS0tLS0K</prv>

4261      </cert>
4262
4263      <revision>
4264          <time>1493217875</time>
4265          <description><![CDATA[admin@10.97.67.148: /firewall_nat_1to1_edit.php
made unknown change]]></description>
4266          <username>admin@10.97.67.148</username>
4267      </revision>
4268      <gateways>
4269          <gateway_item>
4270              <interface>wan</interface>
4271              <gateway>10.33.50.33</gateway>
4272              <name>GW_WAN</name>
4273              <weight>1</weight>
4274              <ipprotocol>inet</ipprotocol>
4275              <interval/>
4276              <descr><![CDATA[Interface wan Gateway]]></descr>
4277              <defaultgw/>
4278          </gateway_item>
4279          <gateway_item>
4280              <interface>lan</interface>

```

```
4281      <gateway>192.168.13.14</gateway>
4282      <name>VLAN2014</name>
4283      <weight>1</weight>
4284      <ipprotocol>inet</ipprotocol>
4285      <descr/>
4286      </gateway_item>
4287      <gateway_item>
4288          <interface>lan</interface>
4289          <gateway>192.168.13.19</gateway>
4290          <name>VLAN2019</name>
4291          <weight>1</weight>
4292          <ipprotocol>inet</ipprotocol>
4293          <descr><! [CDATA[VLAN2019]]></descr>
4294      </gateway_item>
4295      <gateway_item>
4296          <interface>lan</interface>
4297          <gateway>192.168.13.18</gateway>
4298          <name>VLAN2018</name>
4299          <weight>1</weight>
4300          <ipprotocol>inet</ipprotocol>
4301          <descr><! [CDATA[VLAN2018]]></descr>
4302      </gateway_item>
4303      <gateway_item>
4304          <interface>lan</interface>
4305          <gateway>192.168.13.15</gateway>
4306          <name>VLAN2015</name>
4307          <weight>1</weight>
4308          <ipprotocol>inet</ipprotocol>
4309          <descr/>
4310      </gateway_item>
4311      <gateway_item>
4312          <interface>lan</interface>
4313          <gateway>192.168.13.16</gateway>
4314          <name>VLAN2016</name>
```

```
4315          <weight>1</weight>
4316          <ipprotocol>inet</ipprotocol>
4317          <descr/>
4318          </gateway_item>
4319          <gateway_item>
4320          <interface>lan</interface>
4321          <gateway>192.168.13.17</gateway>
4322          <name>VLAN2017</name>
4323          <weight>1</weight>
4324          <ipprotocol>inet</ipprotocol>
4325          <descr/>
4326          </gateway_item>
4327          <gateway_item>
4328          <interface>lan</interface>
4329          <gateway>192.168.13.20</gateway>
4330          <name>VLAN2020</name>
4331          <weight>1</weight>
4332          <ipprotocol>inet</ipprotocol>
4333          <descr/>
4334          </gateway_item>
4335          <gateway_item>
4336          <interface>lan</interface>
4337          <gateway>192.168.13.10</gateway>
4338          <name>VLAN2066</name>
4339          <weight>1</weight>
4340          <ipprotocol>inet</ipprotocol>
4341          <descr><! [CDATA[Gateway to Vendor Net] ]></descr>
4342          </gateway_item>
4343        </gateways>
4344        <ppps/>
4345        <dyndnses/>
4346        <virtualip>
4347          <vip>
4348            <mode>ipalias</mode>
```

```
4349      <interface>wan</interface>
4350      <unqid>576b23658af3d</unqid>
4351      <descr><! [CDATA[Virtual IP for Splunk] ]></descr>
4352      <type>single</type>
4353      <subnet_bits>32</subnet_bits>
4354      <subnet>10.33.50.35</subnet>
4355      </vip>
4356      <vip>
4357          <mode>ipalias</mode>
4358          <interface>wan</interface>
4359          <unqid>5773d4c39ae54</unqid>
4360          <descr><! [CDATA[Virtual IP for RadiantOne VDS] ]></descr>
4361          <type>single</type>
4362          <subnet_bits>32</subnet_bits>
4363          <subnet>10.33.50.37</subnet>
4364      </vip>
4365      <vip>
4366          <mode>ipalias</mode>
4367          <interface>wan</interface>
4368          <unqid>57a8ce7868f78</unqid>
4369          <descr><! [CDATA[Virtual IP for Hytrust ESXi Server] ]></descr>
4370          <type>single</type>
4371          <subnet_bits>32</subnet_bits>
4372          <subnet>10.33.50.36</subnet>
4373      </vip>
4374      <vip>
4375          <mode>ipalias</mode>
4376          <interface>wan</interface>
4377          <unqid>57aa0a0a09a4d09</unqid>
4378          <descr><! [CDATA[VIP for Hytrust CloudControl VM] ]></descr>
4379          <type>single</type>
4380          <subnet_bits>32</subnet_bits>
4381          <subnet>10.33.50.38</subnet>
4382      </vip>
```

```
4383      <vip>
4384          <mode>ipalias</mode>
4385          <interface>wan</interface>
4386          <unqid>57b615eac1f16</unqid>
4387          <descr><! [CDATA[VIP for VCenter Server]]></descr>
4388          <type>single</type>
4389          <subnet_bits>32</subnet_bits>
4390          <subnet>10.33.50.39</subnet>
4391      </vip>
4392      <vip>
4393          <mode>ipalias</mode>
4394          <interface>wan</interface>
4395          <unqid>57bd089e9ab62</unqid>
4396          <descr><! [CDATA[VIP for ActiveDirectory]]></descr>
4397          <type>single</type>
4398          <subnet_bits>32</subnet_bits>
4399          <subnet>10.33.50.40</subnet>
4400      </vip>
4401      <vip>
4402          <mode>ipalias</mode>
4403          <interface>wan</interface>
4404          <unqid>57bf0bbc594c5</unqid>
4405          <descr><! [CDATA[VIP for OpenLDAP]]></descr>
4406          <type>single</type>
4407          <subnet_bits>32</subnet_bits>
4408          <subnet>10.33.50.41</subnet>
4409      </vip>
4410      <vip>
4411          <mode>ipalias</mode>
4412          <interface>wan</interface>
4413          <unqid>57bf97481ae8c</unqid>
4414          <descr><! [CDATA[VIP for Internal Pfsense Firewalls]]></descr>
4415          <type>single</type>
4416          <subnet_bits>32</subnet_bits>
```

```
4417          <subnet>10.33.50.42</subnet>
4418      </vip>
4419      <vip>
4420          <mode>ipalias</mode>
4421          <interface>wan</interface>
4422          <unqid>581788c622d42</unqid>
4423          <descr><! [CDATA[VIP for ConsoleWorks -- Mapping to Internal
4424 Address]]></descr>
4425          <type>single</type>
4426          <subnet_bits>32</subnet_bits>
4427          <subnet>10.33.50.43</subnet>
4428      </vip>
4429      <vip>
4430          <mode>ipalias</mode>
4431          <interface>wan</interface>
4432          <unqid>58179833f127e</unqid>
4433          <descr><! [CDATA[Testing ]]></descr>
4434          <type>single</type>
4435          <subnet_bits>32</subnet_bits>
4436          <subnet>10.33.50.44</subnet>
4437      </vip>
4438      <vip>
4439          <mode>ipalias</mode>
4440          <interface>wan</interface>
4441          <unqid>58e410a9241f1</unqid>
4442          <descr><! [CDATA[Mapping to CentOSToAD VM (test machine) ]]></descr>
4443          <type>single</type>
4444          <subnet_bits>32</subnet_bits>
4445          <subnet>10.33.50.45</subnet>
4446      </vip>
4447      <vip>
4448          <mode>ipalias</mode>
4449          <interface>wan</interface>
4450          <unqid>5900b1ef3b079</unqid>
```

```
4451             <descr><! [CDATA[AlertEnterprise Enterprise Guardian]]></descr>
4452             <type>single</type>
4453             <subnet_bits>32</subnet_bits>
4454             <subnet>10.33.50.46</subnet>
4455         </vip>
4456     </virtualip>
4457 </pfSense>
```

## 2.10.2 Firewall Configuration for Common Services Subnet

```
4458 <?xml version="1.0"?>
4459 <pfSense>
4460     <version>15.4</version>
4461     <lastchange/>
4462     <theme>pfSense_ng</theme>
4463     <system>
4464         <optimization>normal</optimization>
4465         <hostname>FS-ARM</hostname>
4466         <domain>FS-ARM.gov</domain>
4467         <group>
4468             <name>all</name>
4469             <description><! [CDATA[All Users]]></description>
4470             <scope>system</scope>
4471             <gid>1998</gid>
4472             <member>0</member>
4473         </group>
4474         <group>
4475             <name>admins</name>
4476             <description><! [CDATA[System Administrators]]></description>
4477             <scope>system</scope>
4478             <gid>1999</gid>
4479             <member>0</member>
4480             <priv>page-all</priv>
4481         </group>
4482         <user>
4483             <name>admin</name>
```

```
4485      <descr><! [CDATA[System Administrator]]></descr>
4486      <scope>system</scope>
4487      <groupname>admins</groupname>
4488      <password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
4489      <uid>0</uid>
4490      <priv>user-shell-access</priv>
4491    </user>
4492    <nextuid>2000</nextuid>
4493    <nextgid>2000</nextgid>
4494    <timezone>America/New_York</timezone>
4495    <time-update-interval/>
4496    <timeservers>10.97.74.8</timeservers>
4497    <webgui>
4498      <protocol>http</protocol>
4499      <loginautocomplete/>
4500      <ssl-certref>5720a0502b277</ssl-certref>
4501      <dashboardcolumns>2</dashboardcolumns>
4502      <port/>
4503      <max_procs>2</max_procs>
4504      <nohttppreferercheck/>
4505    </webgui>
4506    <disablenatreflection>yes</disablenatreflection>
4507    <disablesegmentationoffloading/>
4508    <disablelargereceiveoffloading/>
4509    <ipv6allow/>
4510    <powerd_ac_mode>hadp</powerd_ac_mode>
4511    <powerd_battery_mode>hadp</powerd_battery_mode>
4512    <powerd_normal_mode>hadp</powerd_normal_mode>
4513    <bogons>
4514      <interval>monthly</interval>
4515    </bogons>
4516    <language>en_US</language>
4517    <dns1gw>GW_WAN</dns1gw>
4518    <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/>
```

```
4553             <track6-interface>wan</track6-interface>
4554             <track6-prefix-id>0</track6-prefix-id>
4555             <gateway/>
4556             <gatewayv6/>
4557         </lan>
4558     </interfaces>
4559     <staticroutes>
4560         <route>
4561             <network>192.168.17.0/24</network>
4562             <gateway>GW_VLAN17</gateway>
4563             <descr><! [CDATA[Route to VLAN 17]]></descr>
4564         </route>
4565     </staticroutes>
4566     <dhcpd>
4567         <lan>
4568             <enable/>
4569             <range>
4570                 <from>192.168.19.100</from>
4571                 <to>192.168.19.150</to>
4572             </range>
4573         </lan>
4574         <opt1>
4575             <enable/>
4576             <range>
4577                 <from>192.168.14.100</from>
4578                 <to>192.168.14.150</to>
4579             </range>
4580         </opt1>
4581         <opt2>
4582             <enable/>
4583             <range>
4584                 <from>192.168.15.100</from>
4585                 <to>192.168.15.150</to>
4586             </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/>
```

```
4621          <tagged/>
4622          <direction>any</direction>
4623          <quick>yes</quick>
4624          <floating>yes</floating>
4625          <max/>
4626          <max-src-nodes/>
4627          <max-src-conn/>
4628          <max-src-states/>
4629          <statetimeout/>
4630          <statetype>keep state</statetype>
4631          <os/>
4632          <protocol>tcp/udp</protocol>
4633          <source>
4634          <any/>
4635        </source>
4636          <destination>
4637          <network>lan</network>
4638        </destination>
4639        <descr><![CDATA[Allow Any to LAN net]]></descr>
4640        <updated>
4641          <time>1493319263</time>
4642          <username>admin@10.97.67.143</username>
4643        </updated>
4644        <created>
4645          <time>1493319263</time>
4646          <username>admin@10.97.67.143</username>
4647        </created>
4648        <disabled/>
4649      </rule>
4650      <rule>
4651        <id/>
4652        <tracker>1481038226</tracker>
4653        <type>pass</type>
4654        <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/>
```

```
4723      <tracker>1493314739</tracker>
4724      <type>pass</type>
4725      <interface>wan</interface>
4726      <ipprotocol>inet</ipprotocol>
4727      <tag/>
4728      <tagged/>
4729      <direction>any</direction>
4730      <quick>yes</quick>
4731      <floating>yes</floating>
4732      <max/>
4733      <max-src-nodes/>
4734      <max-src-conn/>
4735      <max-src-states/>
4736      <statetimeout/>
4737      <statetype>keep state</statetype>
4738      <os/>
4739      <protocol>tcp/udp</protocol>
4740      <source>
4741          <any/>
4742      </source>
4743      <destination>
4744          <any/>
4745          <port>636</port>
4746      </destination>
4747      <descr><! [CDATA[Allow Connection to LDAPS on AD and
4748 OpenLDAP]]></descr>
4749      <created>
4750          <time>1493314739</time>
4751          <username>admin@10.97.67.143</username>
4752      </created>
4753      <updated>
4754          <time>1493319543</time>
4755          <username>admin@10.97.67.143</username>
4756      </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 between]]></descr>
4786          <created>
4787              <time>1472179541</time>
4788              <username>admin@192.168.13.135</username>
4789          </created>
4790          <updated>
```

```
4791                  <time>1493311684</time>
4792                  <username>admin@10.97.67.143</username>
4793              </updated>
4794          </rule>
4795      <rule>
4796          <id/>
4797          <tracker>1493327079</tracker>
4798          <type>pass</type>
4799          <interface>wan</interface>
4800          <ipprotocol>inet</ipprotocol>
4801          <tag/>
4802          <tagged/>
4803          <direction>any</direction>
4804          <quick>yes</quick>
4805          <floating>yes</floating>
4806          <max/>
4807          <max-src-nodes/>
4808          <max-src-conn/>
4809          <max-src-states/>
4810          <statetimeout/>
4811          <statetype>keep state</statetype>
4812          <os/>
4813          <protocol>icmp</protocol>
4814          <source>
4815              <any/>
4816          </source>
4817          <destination>
4818              <network>lan</network>
4819          </destination>
4820          <descr><! [CDATA[Allow ICMP for troubleshooting]]></descr>
4821          <updated>
4822              <time>1493327079</time>
4823              <username>admin@10.97.67.143</username>
4824          </updated>
```

```
4825          <created>
4826              <time>1493327079</time>
4827              <username>admin@10.97.67.143</username>
4828          </created>
4829      </rule>
4830      <rule>
4831          <id/>
4832          <tracker>1493327306</tracker>
4833          <type>pass</type>
4834          <interface>wan</interface>
4835          <ipprotocol>inet</ipprotocol>
4836          <tag/>
4837          <tagged/>
4838          <direction>any</direction>
4839          <quick>yes</quick>
4840          <floating>yes</floating>
4841          <max/>
4842          <max-src-nodes/>
4843          <max-src-conn/>
4844          <max-src-states/>
4845          <statetimeout/>
4846          <statetype>keep state</statetype>
4847          <os></os>
4848          <protocol>tcp/udp</protocol>
4849          <source>
4850              <any/>
4851          </source>
4852          <destination>
4853              <any/>
4854              <port>53</port>
4855          </destination>
4856          <descr><! [CDATA[Allow DNS Requests to AD]]></descr>
4857          <updated>
4858              <time>1493327306</time>
```

```
4859             <username>admin@10.97.67.143</username>
4860         </updated>
4861         <created>
4862             <time>1493327306</time>
4863             <username>admin@10.97.67.143</username>
4864         </created>
4865     </rule>
4866     <rule>
4867         <id/>
4868         <tracker>1493312171</tracker>
4869         <type>pass</type>
4870         <interface>wan</interface>
4871         <ipprotocol>inet</ipprotocol>
4872         <tag/>
4873         <tagged/>
4874         <max/>
4875         <max-src-nodes/>
4876         <max-src-conn/>
4877         <max-src-states/>
4878         <statetimeout/>
4879         <statetype>keep state</statetype>
4880         <os/>
4881         <protocol>tcp</protocol>
4882         <source>
4883             <any/>
4884         </source>
4885         <destination>
4886             <network>lan</network>
4887             <port>389</port>
4888         </destination>
4889         <descr><! [CDATA[Allow LDAP traffic to LAN nodes]]></descr>
4890         <updated>
4891             <time>1493312171</time>
4892             <username>admin@10.97.67.143</username>
```

```
4893          </updated>
4894          <created>
4895              <time>1493312171</time>
4896              <username>admin@10.97.67.143</username>
4897          </created>
4898      </rule>
4899      <rule>
4900          <id/>
4901          <tracker>1493313314</tracker>
4902          <type>pass</type>
4903          <interface>wan</interface>
4904          <ipprotocol>inet</ipprotocol>
4905          <tag/>
4906          <tagged/>
4907          <max/>
4908          <max-src-nodes/>
4909          <max-src-conn/>
4910          <max-src-states/>
4911          <statetimeout/>
4912          <statetype>keep state</statetype>
4913          <os/>
4914          <protocol>tcp/udp</protocol>
4915          <source>
4916              <any/>
4917          </source>
4918          <destination>
4919              <network>lan</network>
4920              <port>53</port>
4921          </destination>
4922          <descr><! [CDATA[Allow DNS traffic to LAN nodes] ]></descr>
4923          <updated>
4924              <time>1493313314</time>
4925              <username>admin@10.97.67.143</username>
4926          </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>
```

```
4961          <time>1493312231</time>
4962          <username>admin@10.97.67.143</username>
4963      </created>
4964  </rule>
4965  <rule>
4966      <id/>
4967      <tracker>1493311864</tracker>
4968      <type>pass</type>
4969      <interface>wan</interface>
4970      <ipprotocol>inet</ipprotocol>
4971      <tag/>
4972      <tagged/>
4973      <max/>
4974      <max-src-nodes/>
4975      <max-src-conn/>
4976      <max-src-states/>
4977      <statetimeout/>
4978      <statetype>keep state</statetype>
4979      <os/>
4980      <protocol>tcp</protocol>
4981      <source>
4982          <any/>
4983      </source>
4984      <destination>
4985          <network>lan</network>
4986          <port>22</port>
4987      </destination>
4988      <descr><! [CDATA[Allow SSH traffic to LAN nodes ]]></descr>
4989      <updated>
4990          <time>1493311864</time>
4991          <username>admin@10.97.67.143</username>
4992      </updated>
4993      <created>
4994          <time>1493311864</time>
```

```
4995             <username>admin@10.97.67.143</username>
4996         </created>
4997     </rule>
4998     <rule>
4999         <id/>
5000         <tracker>1493311502</tracker>
5001         <type>pass</type>
5002         <interface>wan</interface>
5003         <ipprotocol>inet</ipprotocol>
5004         <tag/>
5005         <tagged/>
5006         <max/>
5007         <max-src-nodes/>
5008         <max-src-conn/>
5009         <max-src-states/>
5010         <statetimeout/>
5011         <statetype>keep state</statetype>
5012         <os/>
5013         <protocol>tcp/udp</protocol>
5014         <source>
5015             <network>lan</network>
5016         </source>
5017         <destination>
5018             <any/>
5019         </destination>
5020         <descr><! [CDATA[Allow all LAN traffic to go to anywhere --Applied
5021 to ]]></descr>
5022         <updated>
5023             <time>1493311502</time>
5024             <username>admin@10.97.67.143</username>
5025         </updated>
5026         <created>
5027             <time>1493311502</time>
5028             <username>admin@10.97.67.143</username>
```

```
5029          </created>
5030      </rule>
5031      <rule>
5032          <id/>
5033          <tracker>1493311408</tracker>
5034          <type>pass</type>
5035          <interface>wan</interface>
5036          <ipprotocol>inet</ipprotocol>
5037          <tag/>
5038          <tagged/>
5039          <max/>
5040          <max-src-nodes/>
5041          <max-src-conn/>
5042          <max-src-states/>
5043          <statetimeout/>
5044          <statetype>keep state</statetype>
5045          <os/>
5046          <protocol>tcp</protocol>
5047          <source>
5048              <any/>
5049          </source>
5050          <destination>
5051              <network>wanip</network>
5052              <port>80</port>
5053          </destination>
5054          <descr><! [CDATA[Allow to Port 80 on Firewall WAN] ]></descr>
5055          <updated>
5056              <time>1493311408</time>
5057              <username>admin@10.97.67.143</username>
5058          </updated>
5059          <created>
5060              <time>1493311408</time>
5061              <username>admin@10.97.67.143</username>
5062          </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>
```

```
5131          <id/>
5132          <tracker>1469127156</tracker>
5133          <type>pass</type>
5134          <interface>wan</interface>
5135          <ipprotocol>inet</ipprotocol>
5136          <tag/>
5137          <tagged/>
5138          <max/>
5139          <max-src-nodes/>
5140          <max-src-conn/>
5141          <max-src-states/>
5142          <statetimeout/>
5143          <statetype>keep state</statetype>
5144          <os/>
5145          <protocol>tcp/udp</protocol>
5146          <source>
5147          <any/>
5148        </source>
5149          <destination>
5150          <any/>
5151        </destination>
5152          <disabled/>
5153          <descr/>
5154          <created>
5155          <time>1469127156</time>
5156          <username>admin@192.168.13.132</username>
5157        </created>
5158          <updated>
5159          <time>1493311628</time>
5160          <username>admin@10.97.67.143</username>
5161        </updated>
5162      </rule>
5163      <rule>
5164          <id/>
```

```
5165             <tracker>1480964347</tracker>
5166             <type>pass</type>
5167             <interface>wan</interface>
5168             <ipprotocol>inet</ipprotocol>
5169             <tag/>
5170             <tagged/>
5171             <max/>
5172             <max-src-nodes/>
5173             <max-src-conn/>
5174             <max-src-states/>
5175             <statetimeout/>
5176             <statetype>keep state</statetype>
5177             <os/>
5178             <source>
5179                 <address>192.168.14.111</address>
5180             </source>
5181             <destination>
5182                 <any/>
5183             </destination>
5184             <disabled/>
5185             <descr><![CDATA[Allow Radiant (192.168.14.111) to Get Subnet 19
5186 with]]></descr>
5187             <created>
5188                 <time>1480964347</time>
5189                 <username>admin@10.97.67.144</username>
5190             </created>
5191             <updated>
5192                 <time>1493311596</time>
5193                 <username>admin@10.97.67.143</username>
5194             </updated>
5195         </rule>
5196         <rule>
5197             <id/>
5198             <tracker>1480964466</tracker>
```

```
5199          <type>pass</type>
5200          <interface>wan</interface>
5201          <ipprotocol>inet</ipprotocol>
5202          <tag/>
5203          <tagged/>
5204          <max/>
5205          <max-src-nodes/>
5206          <max-src-conn/>
5207          <max-src-states/>
5208          <statetimeout/>
5209          <statetype>keep state</statetype>
5210          <os/>
5211          <source>
5212              <address>192.168.17.100</address>
5213          </source>
5214          <destination>
5215              <any/>
5216          </destination>
5217          <disabled/>
5218          <descr><! [CDATA[Allow Radiant (192.168.17.100) to Get Subnet 19
5219 from] ]></descr>
5220          <created>
5221              <time>1480964466</time>
5222              <username>admin@10.97.67.144</username>
5223          </created>
5224          <updated>
5225              <time>1493311572</time>
5226              <username>admin@10.97.67.143</username>
5227          </updated>
5228      </rule>
5229      <rule>
5230          <id/>
5231          <tracker>1465935224</tracker>
5232          <type>pass</type>
```

```
5233             <interface>wan</interface>
5234             <ipprotocol>inet</ipprotocol>
5235             <tag/>
5236             <tagged/>
5237             <max/>
5238             <max-src-nodes/>
5239             <max-src-conn/>
5240             <max-src-states/>
5241             <statetimeout/>
5242             <statetype>keep state</statetype>
5243             <os/>
5244             <protocol>icmp</protocol>
5245             <source>
5246                 <any/>
5247             </source>
5248             <destination>
5249                 <any/>
5250             </destination>
5251             <descr/>
5252             <updated>
5253                 <time>1465935224</time>
5254                 <username>admin@192.168.18.100</username>
5255             </updated>
5256             <created>
5257                 <time>1465935224</time>
5258                 <username>admin@192.168.18.100</username>
5259             </created>
5260         </rule>
5261         <rule>
5262             <id/>
5263             <tracker>1469127171</tracker>
5264             <type>pass</type>
5265             <interface>lan</interface>
5266             <ipprotocol>inet</ipprotocol>
```

```
5267          <tag/>
5268          <tagged/>
5269          <max/>
5270          <max-src-nodes/>
5271          <max-src-conn/>
5272          <max-src-states/>
5273          <statetimeout/>
5274          <statetype>keep state</statetype>
5275          <os/>
5276          <protocol>tcp/udp</protocol>
5277          <source>
5278          <any/>
5279          </source>
5280          <destination>
5281          <any/>
5282          </destination>
5283          <disabled/>
5284          <descr/>
5285          <created>
5286          <time>1469127171</time>
5287          <username>admin@192.168.13.132</username>
5288          </created>
5289          <updated>
5290          <time>1493322054</time>
5291          <username>admin@10.97.67.143</username>
5292          </updated>
5293          </rule>
5294          <rule>
5295          <id/>
5296          <tracker>1465935241</tracker>
5297          <type>pass</type>
5298          <interface>lan</interface>
5299          <ipprotocol>inet</ipprotocol>
5300          <tag/>
```

```
5301          <tagged/>
5302          <max/>
5303          <max-src-nodes/>
5304          <max-src-conn/>
5305          <max-src-states/>
5306          <statetimeout/>
5307          <statetype>keep state</statetype>
5308          <os/>
5309          <protocol>icmp</protocol>
5310          <source>
5311          <any/>
5312        </source>
5313          <destination>
5314          <any/>
5315        </destination>
5316          <descr/>
5317          <updated>
5318          <time>1465935241</time>
5319          <username>admin@192.168.18.100</username>
5320        </updated>
5321          <created>
5322          <time>1465935241</time>
5323          <username>admin@192.168.18.100</username>
5324        </created>
5325      </rule>
5326      <rule>
5327          <type>pass</type>
5328          <ipprotocol>inet</ipprotocol>
5329          <descr><! [CDATA[Default allow LAN to any rule] ]></descr>
5330          <interface>lan</interface>
5331          <tracker>0100000101</tracker>
5332          <source>
5333          <network>lan</network>
5334        </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>
```

```
5404          <minute>1</minute>
5405          <hour>1</hour>
5406          <mday>*</mday>
5407          <month>*</month>
5408          <wday>*</wday>
5409          <who>root</who>
5410          <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
5411      </item>
5412      <item>
5413          <minute>*/60</minute>
5414          <hour>*</hour>
5415          <mday>*</mday>
5416          <month>*</month>
5417          <wday>*</wday>
5418          <who>root</who>
5419          <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
5420 virusprot</command>
5421      </item>
5422      <item>
5423          <minute>30</minute>
5424          <hour>12</hour>
5425          <mday>*</mday>
5426          <month>*</month>
5427          <wday>*</wday>
5428          <who>root</who>
5429          <command>/usr/bin/nice -n20 /etc/rc.update_urllables</command>
5430      </item>
5431  </cron>
5432  <wol/>
5433  <rrd>
5434      <enable/>
5435  </rrd>
5436  <load_balancer>
5437      <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>
```

```
5472      <descr><! [CDATA[Generic SMTP]]></descr>
5473      <options>
5474          <send/>
5475          <expect>220 *</expect>
5476      </options>
5477      </monitor_type>
5478  </load_balancer>
5479  <widgets>
5480      <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
5482 /sequence>
5483      </widgets>
5484  <openvpn/>
5485  <dnshaper>
5486  </dnshaper>
5487  <unbound>
5488      <enable/>
5489      <dnssec/>
5490      <active_interface/>
5491      <outgoing_interface/>
5492      <custom_options/>
5493      <hideidentity/>
5494      <hideversion/>
5495      <dnssecstripped/>
5496  </unbound>
5497  <dhcpdv6>
5498      <lan>
5499          <range>
5500              <from>::1000</from>
5501              <to>::2000</to>
5502          </range>
5503          <ramode>assist</ramode>
5504          <rapriority>medium</rapriority>
5505      </lan>
5506  </dhcpdv6>
```

```

5507      <cert>
5508          <refid>5720a0502b277</refid>
5509          <descr><![CDATA[webConfigurator default (5720a0502b277) ]]></descr>
5510          <type>server</type>
5511          <crt>LS0tLS1CRUdJTibDRVJUSUZJQ0FURS0tLS0tck1JSUziVENDQkZXZ0F3SUJBZ01CQURBTkJna3
5512 Foa21HOXcwQkFRc0ZBRENcDERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnT1ZCQWdUQ1ZOMF1YUmxFNUkV3RHdZ
5513 RFZRUUhf2hNYjJoaGJhbDB1VEU0TURZ0ExVUVDAe12Y0daVApaVzV6W1NCM1pXSkRiMjVtYVdkMWntRjBiM0
5514 1nVTJWc1ppMVRhV2R1WldRZ1EyVnlkR2xtYVdOaGRHVxhLREFtCkJna3Foa21HOXcwQkNRRVdHV0ZrYldsdVFI
5515 Qm1VmlZ1YzJvdWJHOpwZV3hrYjIxaGFVNHHlakFjQmdOVkJBTVQKRLhCbVUyVnVjM1V0T1RjeU1HRxdOVEF5WW
5516 pJM056QWVGdzB4TmpBME1qY3hNEU1TkRSYUZ3M1NVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
5517 d0pWVXpFT01Bd0dBMVVFQ0JNR1UzUmhkR1V4RVBRUEJnT1ZCQWNUCKNFehZMZMkZzYVhSNU1Uz3dOZ11EV1FRS0
5518 V50XdabE5sYm5ObE1IZGxza052Ym1acFozVn1ZWFJ2Y21CVFpXeG0KTFZ0cFoyNWxaQ0JEWlhKMGFxWnBZMkYw
5519 W1Rfb01DWUDDU3FHU01iM0RRRUpBU1aWVdSdGFXNUFjR1pUW1clegpaUzVzYjJoaGJHUnZiV0ZwYmpFZU1Cd0
5520 dBMVVFQXhNVmNHW1RaVzV6W1MwMU56SXdZVEEXTURKaU1qYzNNSU1CCk1qQU5CZ2txaGtpRz13MEJBUVGQUFP
5521 Q0FROEFNSU1CQ2dLQ0FRRUF0L085aD1nT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGjsQ2NWCgJNYXFmUE1aVzNMdG
5522 hDODBH0dhZnJENWdqctrwZkNNMH1zbEFPPaV1ZK1hDYjdnA2o0dmtTMgpmbz14emNyaDurNv1aY1BHeXR1a2ls
5523 ZWR4bjFWef16S11zYXZKdn1Kb11RMctNTkx0dkFjYnRhTUfOzjh1ZkRFC1hrc1NVQ0N5YTfrbEYxNWJGZmcyUG
5524 E0eGRvMk9PNUJ5RzBrv0NKU2o4K1R1WhVkuFRJTkx3QUZnd1E5K1BQZkwKVTQxMFbVb3FFbWEwdzU4Q1RZKzZh
5525 ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29EN1oxQmdCUApyeXd1SEZwd3J1LytyWEExieEcrcD
5526 dwYXI0aHR0UFRDcm11NmFqQVVTNmpvN05kOE1QNPzZ1kzR0h2ZjhZUU1ECKfRQUJvNE1CaGpDQ0FZSXdDUV1E
5527 V1IwVEJBSxDbREFSQmdsZ2hrZ0JodmhDQVFFRJBTUNCa0F3TxDZS11JWkkQV1iNFFnRU5CQ11XskU5d1pXNV
5528 RVIMHdnUjJwdVpYSmhkr1ZrSUZobGNuWmxjaUJEWlhKMGFxWnBZMkYwW1RBZApCZ05WSFE0RUznuVU3K11LRmNp
5529 OFFVSGhTZ0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K11LCkZjaThRVUh0u2dMRHY4RUNzY0
5530 Nkd0FLaGdicWtnYmN3Z2JReEN6QuPCz05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
5531 VUVCeE1JVec5allXeHBkSGt4T0RBMkJnT1ZCQW9UDTNCbVuYvNjM1VnZDJWaQpRmj11Wm1sbmRYSmhkRz15SU
5532 ZOBGJHWXRVMmxuYm1Wa01FTmxjblJwWm1sa11YUmNxU2d3SmdSktvWk1lodmNOCKFRa0JGaGx0WkcxcGJrQnda
5533 bE5sYm5ObExteHZZMkzzWkc5dF1XbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
5534 56ZUNBUUF3SFFZRFZSMGxCQ113RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UVBd01G
5535 b0RBTkJna3Foa21HOXcwQkFRc0ZBQU9DQVFFQXjzFpQdXd2MVzuUC82NmJDWFJ5CkVmaW1LRw1PcmtNaTB5M0
5536 9PwgTzWEs1cEM2dTd6Uk13WjEvRjYyRUp3OD1UOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWjhRu42NEkxOHFud3Zm
5537 S2JrREZvRThMR1hSdzBkMnAyTGVmYtd4YTIVsGNHc0xHTktPbkjxb3N4ejUrQ1B3ZwpWeVraTs9wV3p3aDdQRG
5538 c4bGdrcVc3dSt1b01DNDJ1bVjkOURCTmlzdfJ4Rv1NmKfLQkFszG1LYStvRUY1VUuwCm43aXpvN1Z4dHJWMTJv
5539 TTdyS11RQ05kY00xZkvSeUwvb3ZkUnVpa0F5Wm1VvnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOvpPSmR2QmZLVU
5540 1sUW1ELyswSVpTaFxRdczWkdsaaHtK2t0eWc1aDjhUjUwYjh3Wm9zQnNjSUZDa0pFbpg0UT09Ci0tLS0tRU5E
5541 IENFU1RJRK1DQVRFLS0tLS0K</crt>
5542
5543 <prv>LS0tLS1CRUdJTibQk1wQVRFIetFWS0tLS0tck1JSUV2Z01CQURBTkJna3Foa21HOXcwQkFRRU
5544 ZBQVNDQktnD2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M01hY1kKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4
5545 eGxiY3UyRUX6UvpJWnArc1BtQ09yaWw4SxpUS31VQTZKaGo1YwpKdnN5U1BpK1JMWitqM0h0eXVIBjdsaxGzOG
5546 JLMjZTS1Y1M0dmV1hGak1saXhxOG0vSw1oaERUNHcwdTI4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEpyV1NVWFhs
5547 c1YrRFk5cmpGMmpZNDrSE1i1U1JZSWxLUHo1TzVtNTA5TWCwdkEKQVdEQkQzNDg50Hrua1hROVNpb1NaclREbn
5548 dKTmo3cHAwQnM4Zhh1RDbjL2poUGFWswNkem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
5549 dHZFYjZudWxxdm1HMjA5Tut1SzdwC1CukxxT2pzMTN3Zy9tT31CCmpjWWU5L314QwdNQkFBrunnZ0VCQUpRRF
5550 pxU3duMnNTUTh0SVNBTVUrvUw0zcxHrb3BzdzB4cWNScmFl0Ed4VmQKejBpOU1KbkzVQWFleTQvL3J1dndhZW1P
5551 R3RYSmZ2ai9jSny3cmJIWGIzYkjtVW9hcDhxY0RjdnhVSm1lHRUZYwQpCL3hjnvpINTlaTuFabWE1VwVQLzNjcd
5552 1zNVhhcHNpc1NXV1I4cFFZc3Z6Mmt6ci8zMXdrQxd4SGJZWHhJVDk1CjNLrmk4VTZUM1hnU1c2eFowZhp1Zn1P
5553 UzAvbXlmN5YlZVoRk1PNmFDc0x1UjZ4N1Rza2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEzdVM0bXdyR2
5554 hMz0NRY1B2MnE5V0Nia0VmNeZUzmRz1ZxchBRNG1ZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZ1F2
5555 YTvgYUgyRm5LdkExR2YxY05hGrVQ2dZrue0NzNMuWoxcExLsmRzn2JxCmtMu3Nvt0Zhtuz1ZG1xU2ttbzh3Qj
5556 1pMxhzB1LQuD0M3U4dtdMz1ztu21ybnMwVvBtmhvRUDryQxmzVFJocEgkUz24VxVsbGvgAktjzK9xRE11TTBC
5557 OGttbFJnUFrmVHPaGnwMGVkamQwK1E5Y2V1Y25kaFp3UE16Tuc3TwRTSApKog5yU2t5TfdMdWuXuvJNzHnbm
5558 NBRDhVYThDZ11FQXpzyjYzbzRBSH1YNjZkcEJ6TG1zYzZxS2d2ZG4xazhVcm02N3RuK2M3NkVhSEtzt1k0Rjdh
5559 S0dFSk1yeU0yQTJTe1Azdm03Rmk4eGrtb1grsx5cUx5t1VwSnZxQ012TVIKRDFpNwvftvvvozvo20UpOK013Sm
5560 Z2RjYrK2tHa1NHOgxan0Vly21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHvtQopJZm1DW1pRSUQ1OENnWUJjamFO
5561 dk5obnFJOG9rWGHBUjR2c3NtNgPwb0tYU1ZScjRIVh05MDFwOGdReXNCWkt0Cn1US2V6VThuUVZvTjNYWmVmBc
5562 8rVEcwYVpKOTZHKy9nNTRWZmZqWTR1elVScHhUt3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3

```

```

5564 QWY5Mi9CbHZJR25FS1pMdnhLWTdVMX1Ib1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpGJNTn
5565 VudmNUUjZxTzR0ekZtdG5TYWN3W1Ftb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
5566 RG1hZGsvKy9Ud2UvVkj1Kbmxx2TW9zs3VjTG42Y1c2eGVhR1hFc3FoUj1hbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
5567 FBamdyQmxrb3pOVnNMZThiWWpkcHR1MVBRs0JnQ0xDR0R1RXNBYUxwZ1RtOG44bgoyQ1h1NE52K113a1Rlczdu
5568 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdyenRCZ1ZLC1UzSThhYnpnUUtwoEwrZj
5569 VadTAxY1pZVk5TU0FIUFRHYm5jb1IzbGVPyjNLeUVXQjdsZFBHQwpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
5570 OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>

5571     </cert>
5572     <revision>
5573         <time>1493327306</time>
5574         <description><! [CDATA[admin@10.97.67.143: /firewall_rules_edit.php made
5575 unknown change]]></description>
5576         <username>admin@10.97.67.143</username>
5577     </revision>
5578     <gateways>
5579         <gateway_item>
5580             <interface>wan</interface>
5581             <gateway>192.168.13.1</gateway>
5582             <name>GW_WAN_2</name>
5583             <weight>1</weight>
5584             <ipprotocol>inet</ipprotocol>
5585             <interval/>
5586             <descr><! [CDATA[Interface wan Gateway] ]></descr>
5587         </gateway_item>
5588         <gateway_item>
5589             <interface>wan</interface>
5590             <gateway>192.168.13.17</gateway>
5591             <name>GW_VLAN17</name>
5592             <weight>1</weight>
5593             <ipprotocol>inet</ipprotocol>
5594             <descr><! [CDATA[Gateway to VLAN 17]]></descr>
5595         </gateway_item>
5596     </gateways>
5597     <ppps/>
5598     <dyndnses/>
5599 </pfSense>

```

### 2.10.3 Firewall Configuration for ID-ARM Subnet

```
5601 <?xml version="1.0"?>
5602 <pfSense>
5603     <version>15.4</version>
5604     <lastchange/>
5605     <theme>pfSense_ng</theme>
5606     <system>
5607         <optimization>normal</optimization>
5608         <hostname>FS-ARM</hostname>
5609         <domain>FS-ARM.gov</domain>
5610         <group>
5611             <name>all</name>
5612             <description><! [CDATA[All Users]]></description>
5613             <scope>system</scope>
5614             <gid>1998</gid>
5615             <member>0</member>
5616         </group>
5617         <group>
5618             <name>admins</name>
5619             <description><! [CDATA[System Administrators]]></description>
5620             <scope>system</scope>
5621             <gid>1999</gid>
5622             <member>0</member>
5623             <priv>page-all</priv>
5624         </group>
5625         <user>
5626             <name>admin</name>
5627             <descr><! [CDATA[System Administrator]]></descr>
5628             <scope>system</scope>
5629             <groupname>admins</groupname>
5630             <password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
5631             <uid>0</uid>
5632             <priv>user-shell-access</priv>
5633         </user>
5634         <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          <nohttppreferercheck/>
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/>
```

```
5737      <range>
5738          <from>192.168.15.100</from>
5739          <to>192.168.15.150</to>
5740      </range>
5741  </opt2>
5742  <opt3>
5743      <enable/>
5744      <range>
5745          <from>192.168.16.100</from>
5746          <to>192.168.16.150</to>
5747      </range>
5748  </opt3>
5749  </dhcpd>
5750  <snmpd>
5751      <syslocation/>
5752      <syscontact/>
5753      <rocommunity>public</rocommunity>
5754  </snmpd>
5755  <diag>
5756      <ipv6nat>
5757          <ipaddr/>
5758      </ipv6nat>
5759  </diag>
5760  <bridge/>
5761  <syslog/>
5762  <nat>
5763      <outbound>
5764          <mode>disabled</mode>
5765      </outbound>
5766  </nat>
5767  <filter>
5768      <rule>
5769          <id/>
5770          <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>
```

```
5805      <id/>
5806      <tracker>1481038086</tracker>
5807      <type>pass</type>
5808      <interface>wan</interface>
5809      <ipprotocol>inet</ipprotocol>
5810      <tag/>
5811      <tagged/>
5812      <direction>any</direction>
5813      <quick>yes</quick>
5814      <floating>yes</floating>
5815      <max/>
5816      <max-src-nodes/>
5817      <max-src-conn/>
5818      <max-src-states/>
5819      <statetimeout/>
5820      <statetype>keep state</statetype>
5821      <os/>
5822      <protocol>tcp/udp</protocol>
5823      <source>
5824          <any/>
5825      </source>
5826      <destination>
5827          <network>lan</network>
5828          <port>2389</port>
5829      </destination>
5830      <descr><! [CDATA[Allow Connection to Radiant Port 2389]]></descr>
5831      <created>
5832          <time>1481038086</time>
5833          <username>admin@10.97.67.155</username>
5834      </created>
5835      <updated>
5836          <time>1493324258</time>
5837          <username>admin@10.97.67.143</username>
5838      </updated>
```

```
5839      </rule>
5840
5841      <rule>
5842          <id/>
5843          <tracker>1493650861</tracker>
5844          <type>pass</type>
5845          <interface>wan</interface>
5846          <ipprotocol>inet</ipprotocol>
5847          <tag/>
5848          <tagged/>
5849          <direction>any</direction>
5850          <quick>yes</quick>
5851          <floating>yes</floating>
5852          <max/>
5853          <max-src-nodes/>
5854          <max-src-conn/>
5855          <max-src-states/>
5856          <statetimeout/>
5857          <statetype>keep state</statetype>
5858          <os/>
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>
```

```
5873                  <username>admin@10.97.67.135</username>
5874          </created>
5875      </rule>
5876      <rule>
5877          <id/>
5878          <tracker>1493650905</tracker>
5879          <type>pass</type>
5880          <interface>wan</interface>
5881          <ipprotocol>inet</ipprotocol>
5882          <tag/>
5883          <tagged/>
5884          <direction>any</direction>
5885          <quick>yes</quick>
5886          <floating>yes</floating>
5887          <max/>
5888          <max-src-nodes/>
5889          <max-src-conn/>
5890          <max-src-states/>
5891          <statetimeout/>
5892          <statetype>keep state</statetype>
5893          <os></os>
5894          <protocol>tcp/udp</protocol>
5895          <source>
5896              <any/>
5897          </source>
5898          <destination>
5899              <network>lan</network>
5900              <port>636</port>
5901          </destination>
5902          <descr><! [CDATA[Allow Connection to Port 636 in LAN]]></descr>
5903          <updated>
5904              <time>1493650905</time>
5905              <username>admin@10.97.67.135</username>
5906          </updated>
```

```
5907             <created>
5908                 <time>1493650905</time>
5909                 <username>admin@10.97.67.135</username>
5910             </created>
5911         </rule>
5912     <rule>
5913         <id/>
5914         <tracker>1493328157</tracker>
5915         <type>pass</type>
5916         <interface>wan</interface>
5917         <ipprotocol>inet</ipprotocol>
5918         <tag/>
5919         <tagged/>
5920         <direction>any</direction>
5921         <quick>yes</quick>
5922         <floating>yes</floating>
5923         <max/>
5924         <max-src-nodes/>
5925         <max-src-conn/>
5926         <max-src-states/>
5927         <statetimeout/>
5928         <statetype>keep state</statetype>
5929         <os/>
5930         <protocol>tcp/udp</protocol>
5931         <source>
5932             <any/>
5933         </source>
5934         <destination>
5935             <network>lan</network>
5936             <port>8089</port>
5937         </destination>
5938         <descr><! [CDATA[Allow Connection to Radiant Port 8089]]></descr>
5939         <updated>
5940             <time>1493328157</time>
```

```
5941                  <username>admin@10.97.67.143</username>
5942              </updated>
5943          <created>
5944              <time>1493328157</time>
5945          <username>admin@10.97.67.143</username>
5946      </created>
5947  </rule>
5948  <rule>
5949      <id/>
5950      <tracker>1493328202</tracker>
5951      <type>pass</type>
5952      <interface>wan</interface>
5953      <ipprotocol>inet</ipprotocol>
5954      <tag/>
5955      <tagged/>
5956      <direction>any</direction>
5957      <quick>yes</quick>
5958      <floating>yes</floating>
5959      <max/>
5960      <max-src-nodes/>
5961      <max-src-conn/>
5962      <max-src-states/>
5963      <statetimeout/>
5964      <statetype>keep state</statetype>
5965      <os/>
5966      <protocol>tcp/udp</protocol>
5967      <source>
5968          <any/>
5969      </source>
5970      <destination>
5971          <network>lan</network>
5972          <port>8090</port>
5973      </destination>
5974      <descr><![CDATA[Allow Connection to Radiant Port 8090]]></descr>
```

```
5975      <updated>
5976          <time>1493328202</time>
5977          <username>admin@10.97.67.143</username>
5978      </updated>
5979      <created>
5980          <time>1493328202</time>
5981          <username>admin@10.97.67.143</username>
5982      </created>
5983  </rule>
5984  <rule>
5985      <id/>
5986      <tracker>1493327695</tracker>
5987      <type>pass</type>
5988      <interface>wan</interface>
5989      <ipprotocol>inet</ipprotocol>
5990      <tag/>
5991      <tagged/>
5992      <direction>any</direction>
5993      <quick>yes</quick>
5994      <floating>yes</floating>
5995      <max/>
5996      <max-src-nodes/>
5997      <max-src-conn/>
5998      <max-src-states/>
5999      <statetimeout/>
6000      <statetype>keep state</statetype>
6001      <os/>
6002      <protocol>tcp/udp</protocol>
6003      <source>
6004          <any/>
6005      </source>
6006      <destination>
6007          <network>lan</network>
6008          <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>
```

```
6043      <network>lan</network>
6044          <port>443</port>
6045      </destination>
6046      <descr><! [CDATA[Allow Connection to Nextlabs port 443]]></descr>
6047      <updated>
6048          <time>1493327739</time>
6049          <username>admin@10.97.67.143</username>
6050      </updated>
6051      <created>
6052          <time>1493327739</time>
6053          <username>admin@10.97.67.143</username>
6054      </created>
6055  </rule>
6056  <rule>
6057      <id/>
6058      <tracker>1493327782</tracker>
6059      <type>pass</type>
6060      <interface>wan</interface>
6061      <ipprotocol>inet</ipprotocol>
6062      <tag/>
6063      <tagged/>
6064      <direction>any</direction>
6065      <quick>yes</quick>
6066      <floating>yes</floating>
6067      <max/>
6068      <max-src-nodes/>
6069      <max-src-conn/>
6070      <max-src-states/>
6071      <statetimeout/>
6072      <statetype>keep state</statetype>
6073      <os/>
6074      <protocol>tcp/udp</protocol>
6075      <source>
6076          <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>
```

```
6111          <source>
6112              <any/>
6113          </source>
6114          <destination>
6115              <any/>
6116              <port>19888</port>
6117          </destination>
6118          <descr><! [CDATA[Allow Connection to Nextlabs port 19888]]></descr>
6119          <updated>
6120              <time>1493327859</time>
6121              <username>admin@10.97.67.143</username>
6122          </updated>
6123          <created>
6124              <time>1493327859</time>
6125              <username>admin@10.97.67.143</username>
6126          </created>
6127      </rule>
6128      <rule>
6129          <id/>
6130          <tracker>1493325919</tracker>
6131          <type>pass</type>
6132          <interface>wan</interface>
6133          <ipprotocol>inet</ipprotocol>
6134          <tag/>
6135          <tagged/>
6136          <direction>any</direction>
6137          <quick>yes</quick>
6138          <floating>yes</floating>
6139          <max/>
6140          <max-src-nodes/>
6141          <max-src-conn/>
6142          <max-src-states/>
6143          <statetimeout/>
6144          <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/>
```

```
6179          <statetype>keep state</statetype>
6180          <os/>
6181          <protocol>tcp/udp</protocol>
6182          <source>
6183              <any/>
6184          </source>
6185          <destination>
6186              <any/>
6187              <port>2000</port>
6188          </destination>
6189          <descr><! [CDATA[Allow Connection to Nextlabs port 2000]]></descr>
6190          <updated>
6191              <time>1493328002</time>
6192              <username>admin@10.97.67.143</username>
6193          </updated>
6194          <created>
6195              <time>1493328002</time>
6196              <username>admin@10.97.67.143</username>
6197          </created>
6198      </rule>
6199      <rule>
6200          <id/>
6201          <tracker>1481037313</tracker>
6202          <type>pass</type>
6203          <interface>wan</interface>
6204          <ipprotocol>inet</ipprotocol>
6205          <tag/>
6206          <tagged/>
6207          <max/>
6208          <max-src-nodes/>
6209          <max-src-conn/>
6210          <max-src-states/>
6211          <statetimeout/>
6212          <statetype>keep state</statetype>
```

```
6213      <os/>
6214      <source>
6215          <address>192.168.14.111</address>
6216      </source>
6217      <destination>
6218          <any/>
6219      </destination>
6220      <descr><! [CDATA[Allow Radiant (192.168.14.111) to get out with any
6221 p]]></descr>
6222      <created>
6223          <time>1481037313</time>
6224          <username>admin@10.97.67.155</username>
6225      </created>
6226      <updated>
6227          <time>1481037359</time>
6228          <username>admin@10.97.67.155</username>
6229      </updated>
6230      <disabled/>
6231      </rule>
6232      <rule>
6233          <id/>
6234          <tracker>1480537443</tracker>
6235          <type>pass</type>
6236          <interface>wan</interface>
6237          <ipprotocol>inet</ipprotocol>
6238          <tag/>
6239          <tagged/>
6240          <max/>
6241          <max-src-nodes/>
6242          <max-src-conn/>
6243          <max-src-states/>
6244          <statetimeout/>
6245          <statetype>keep state</statetype>
6246      <os/>
```

```
6247          <source>
6248              <any/>
6249          </source>
6250          <destination>
6251              <any/>
6252          </destination>
6253          <descr><! [CDATA[Allow Everything]]></descr>
6254          <updated>
6255              <time>1480537443</time>
6256              <username>admin@192.168.13.139</username>
6257          </updated>
6258          <created>
6259              <time>1480537443</time>
6260              <username>admin@192.168.13.139</username>
6261          </created>
6262          <disabled/>
6263      </rule>
6264      <rule>
6265          <id/>
6266          <tracker>1466105351</tracker>
6267          <type>pass</type>
6268          <interface>wan</interface>
6269          <ipprotocol>inet</ipprotocol>
6270          <tag/>
6271          <tagged/>
6272          <max/>
6273          <max-src-nodes/>
6274          <max-src-conn/>
6275          <max-src-states/>
6276          <statetimeout/>
6277          <statetype>keep state</statetype>
6278          <os/>
6279          <protocol>udp</protocol>
6280          <source>
```

```
6281          <any/>
6282      </source>
6283      <destination>
6284          <any/>
6285      </destination>
6286      <descr/>
6287      <updated>
6288          <time>1466105351</time>
6289          <username>admin@192.168.13.101</username>
6290      </updated>
6291      <created>
6292          <time>1466105351</time>
6293          <username>admin@192.168.13.101</username>
6294      </created>
6295      <disabled/>
6296  </rule>
6297  <rule>
6298      <id/>
6299      <tracker>1465934980</tracker>
6300      <type>pass</type>
6301      <interface>wan</interface>
6302      <ipprotocol>inet</ipprotocol>
6303      <tag/>
6304      <tagged/>
6305      <max/>
6306      <max-src-nodes/>
6307      <max-src-conn/>
6308      <max-src-states/>
6309      <statetimeout/>
6310      <statetype>keep state</statetype>
6311      <os/>
6312      <protocol>icmp</protocol>
6313      <source>
6314          <any/>
```

```
6315          </source>
6316          <destination>
6317              <any/>
6318          </destination>
6319          <descr/>
6320          <updated>
6321              <time>1465934980</time>
6322              <username>admin@192.168.14.100</username>
6323          </updated>
6324          <created>
6325              <time>1465934980</time>
6326              <username>admin@192.168.14.100</username>
6327          </created>
6328      </rule>
6329      <rule>
6330          <id/>
6331          <tracker>1461788221</tracker>
6332          <type>pass</type>
6333          <interface>wan</interface>
6334          <ipprotocol>inet</ipprotocol>
6335          <tag/>
6336          <tagged/>
6337          <max/>
6338          <max-src-nodes/>
6339          <max-src-conn/>
6340          <max-src-states/>
6341          <statetimeout/>
6342          <statetype>keep state</statetype>
6343          <os/>
6344          <protocol>tcp</protocol>
6345          <source>
6346              <any/>
6347          </source>
6348          <destination>
```

```
6349          <network>wanip</network>
6350          <port>80</port>
6351      </destination>
6352      <descr><! [CDATA[Allow to Port 80 on Firewall WAN] ]></descr>
6353      <created>
6354          <time>1461788221</time>
6355          <username>admin@192.168.1.2</username>
6356      </created>
6357      <updated>
6358          <time>1493323649</time>
6359          <username>admin@10.97.67.143</username>
6360      </updated>
6361  </rule>
6362  <rule>
6363      <type>pass</type>
6364      <interface>wan</interface>
6365      <ipprotocol>inet</ipprotocol>
6366      <descr><! [CDATA[Easy Rule: Passed from Firewall Log
6367 View]]></descr>
6368      <protocol>udp</protocol>
6369      <source>
6370          <address>192.168.13.101</address>
6371      </source>
6372      <destination>
6373          <address>192.168.13.102</address>
6374          <port>137</port>
6375      </destination>
6376      <created>
6377          <time>1466105470</time>
6378          <username>Easy Rule</username>
6379      </created>
6380  </rule>
6381  <rule>
6382      <id/>
```

```
6383      <tracker>1480537570</tracker>
6384      <type>pass</type>
6385      <interface>lan</interface>
6386      <ipprotocol>inet</ipprotocol>
6387      <tag/>
6388      <tagged/>
6389      <max/>
6390      <max-src-nodes/>
6391      <max-src-conn/>
6392      <max-src-states/>
6393      <statetimeout/>
6394      <statetype>keep state</statetype>
6395      <os/>
6396      <source>
6397          <any/>
6398      </source>
6399      <destination>
6400          <any/>
6401      </destination>
6402      <descr><! [CDATA[All Everything from LAN Interface]]></descr>
6403      <updated>
6404          <time>1480537570</time>
6405          <username>admin@192.168.13.139</username>
6406      </updated>
6407      <created>
6408          <time>1480537570</time>
6409          <username>admin@192.168.13.139</username>
6410      </created>
6411      <disabled/>
6412      </rule>
6413      <rule>
6414          <id/>
6415          <tracker>1466105363</tracker>
6416          <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/>
```

```
6485          <tagged/>
6486          <max/>
6487          <max-src-nodes/>
6488          <max-src-conn/>
6489          <max-src-states/>
6490          <statetimeout/>
6491          <statetype>keep state</statetype>
6492          <os/>
6493          <protocol>tcp</protocol>
6494          <source>
6495          <any/>
6496        </source>
6497          <destination>
6498          <any/>
6499        </destination>
6500        <descr><! [CDATA[Allow Any Any] ]></descr>
6501        <updated>
6502          <time>1465915373</time>
6503          <username>admin@192.168.14.100</username>
6504        </updated>
6505        <created>
6506          <time>1465915373</time>
6507          <username>admin@192.168.14.100</username>
6508        </created>
6509        <disabled/>
6510      </rule>
6511      <rule>
6512        <type>pass</type>
6513        <ipprotocol>inet</ipprotocol>
6514        <descr><! [CDATA[Default allow LAN to any rule] ]></descr>
6515        <interface>lan</interface>
6516        <tracker>0100000101</tracker>
6517        <source>
6518          <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>
```

```
6588          <minute>1</minute>
6589          <hour>1</hour>
6590          <mday>*</mday>
6591          <month>*</month>
6592          <wday>*</wday>
6593          <who>root</who>
6594          <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
6595      </item>
6596      <item>
6597          <minute>*/60</minute>
6598          <hour>*</hour>
6599          <mday>*</mday>
6600          <month>*</month>
6601          <wday>*</wday>
6602          <who>root</who>
6603          <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
6604 virusprot</command>
6605      </item>
6606      <item>
6607          <minute>30</minute>
6608          <hour>12</hour>
6609          <mday>*</mday>
6610          <month>*</month>
6611          <wday>*</wday>
6612          <who>root</who>
6613          <command>/usr/bin/nice -n20 /etc/rc.update_urllables</command>
6614      </item>
6615  </cron>
6616  <wol/>
6617  <rrd>
6618      <enable/>
6619  </rrd>
6620  <load_balancer>
6621      <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>
```

```
6656      <descr><! [CDATA[Generic SMTP]]></descr>
6657      <options>
6658          <send/>
6659          <expect>220 *</expect>
6660      </options>
6661      </monitor_type>
6662      </load_balancer>
6663      <widgets>
6664      <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
6665 /sequence>
6666      </widgets>
6667      <openvpn/>
6668      <dnshaper>
6669      </dnshaper>
6670      <unbound>
6671          <enable/>
6672          <dnssec/>
6673          <active_interface/>
6674          <outgoing_interface/>
6675          <custom_options/>
6676          <hideidentity/>
6677          <hideversion/>
6678          <dnssecstripped/>
6679      </unbound>
6680      </dhcpdv6>
6681          <lan>
6682              <range>
6683                  <from>::1000</from>
6684                  <to>::2000</to>
6685              </range>
6686          </lan>
6687          <ramode>assist</ramode>
6688          <rapriority>medium</rapriority>
6689      </dhcpdv6>
```

```

6691      <cert>
6692          <refid>5720a0502b277</refid>
6693          <descr><![CDATA[webConfigurator default (5720a0502b277) ]]></descr>
6694          <type>server</type>
6695
6696          <crt>LS0tLS1CRUdJTibDRVJUSUZJQ0FURS0tLS0tCk1JSUzivENDQkZXZ0F3SUJBZ01CQURBTkJna3
6697 Foa21HOXcwQkFRc0ZBRENcDERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnT1ZCQWdUQ1ZOMF1YUmxFNUkV3RHdZ
6698 RFZRUUhf2hNYjJoaGJhbDB1VEU0TURZ0ExVUVDAe12Y0daVApaVzV6W1NCM1pXSkRiMjVtYVdkMWNTRjBiM0
6699 1nVTJWc1ppMVRhV2R1WldRZ1EyVnlkR2xtYVdOaGRHVxhLREFtCkJna3Foa21HOXcwQkNRRVdHV0ZrYldsdVFI
6700 Qm1VmlZ1YzJvDwJHOpwZV3hrYjIxagFXNHhIakFjQmdOVkJBTVQKRLhCbVUyVnVjM1V0T1RjeU1HRXdOVEF5WW
6701 pJM056QWVGdzB4TmpBME1qY3hNEU1TkRSYUZ3Mh1NVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
6702 d0pWVXpFT01Bd0dBMVVFQ0JNR1UzUmhkR1V4RVRBUEJnT1ZCQWNNUCKNFehZMZMkZzYVhSNU1Uz3dOZ11EV1FRS0
6703 V5OXdabE5sYm5ObE1IZGxza052Ym1acFozVn1ZWFJ2Y21CVFpXeG0KTFZ0cFoyNWxaQ0JEwlhKMGFxWnBZMkYw
6704 W1Rfb01DWUDDU3FHU01iM0RRRUpBU1aWVdSdGFXNUFjR1pUWlclepgauVzVzYjOaGJHUnziV0ZwYmpFZU1Cd0
6705 dBMVVFQXhNVmNHW1RaVzV6W1MwMU56SXdZVEEXtURKaU1qYzNNSU1CCk1qQU5CZ2txaGtpRz13MEJBUVGQUFP
6706 Q0FROEFNSU1CQ2dLQ0FRRUF0L085aD1nT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGjsQ2NWcGJNYXFmUE1aVzNMdG
6707 hDODBH0dhZnJENwdqctRwZkNNMH1zbEFPPaV1ZK1hDYjdnA2o0dmtTMgpmbz14emNyaDurNv1aY1BHeXR1a2ls
6708 ZWR4bjFWef16S11zYXZKdn1Kb11RMctNTkx0dkFjYnRhTUfOzjh1ZkRFC1hrc1NVQ0N5YTFrbEYxNWJGZmcyUG
6709 E0eGRvMk9PNUJ5RzBrv0NKU2o4K1R1WhVkuFRJTkx3QUZnd1E5K1BQZkwKVTQxMFbVb3FFbWEwdzU4Q1RZKzZh
6710 ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTd1K3IyafZ0N29EN1oxQmdCUApyeXd1SEZwd3J1LytyWEExieEcrcD
6711 dwYXI0aHR0UFRDcm11NmFqQVVTNmpvN05kOE1QNPzZ1kzR0h2ZjhZUU1ECKfFRQUJvNE1CaGpDQ0FZSXdDUV1E
6712 V1IwVEJBSxdBREFSQmdsZ2hrZ0JodmhDQVFFRJBTUNCa0F3TxDZS11JWkkQV1iNFFnRu5CQ11XskU5d1pXNV
6713 RVIMHdnUjJwdVpYSmhkr1ZrSUZobGNuWmxjaUJEwlhKMGFxWnBZMkYwW1RBZApCZ05WSFE0RUznuVU3K11LRmNp
6714 OFFVSGhTZ0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K11LCkZjaThRVUh0u2dMRHY4RUNzY0
6715 Nkd0FLaGdicWtnYmN3Z2JReEN6QuPCz05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
6716 VUVCeE1JVec5allXeHBkSGt4T0RBMkJnT1ZCQW9UDTNCbVuYvNjM1VnZDJWaQpRmj11Wm1sbmRYSmhkRz15SU
6717 ZOBGJHWXRVMmxuYm1Wa01FTmxjblJwWm1sa11YUmnu2d3SmdSktvWk1lodmNOCKFRa0JGaGx0WkcxcGJrQnda
6718 bE5sYm5ObExteHZZMkzzWkc5dF1XbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
6719 56ZUNBUUF3SFFZRFZSMGxCQ113RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd01G
6720 b0RBTkJna3Foa21HOXcwQkFRc0ZBQU9DQVFFQXjzFpQdXd2MVzuUC82NmJDWFJ5CkVmaW1LRw1PcmtNaTB5M0
6721 9PwgTzWEs1cEM2dTd6Uk13WjEvRjYyRUp3OD1UOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWjhRU42NEkxOHFud3Zm
6722 S2JrREZvRThMR1hSdzBkMnAyTGVmYTd4YTIVSGNhC0xHTktPbkjxb3N4ejUrQ1B3ZwpWeVraTS9wV3p3aDdQRG
6723 c4bGdrcVc3dSt1b01DNDJ1bVjkOURCTmlzdfJ4Rv1NmKfLQkFszG1LYStvRUY1VUuwCm43aXpvN1Z4dHJWMTJv
6724 TTdyS11RQ05kY00xZkvSeUwvb3ZkUnVpa0F5Wm1VvnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOvpPSmR2QmZLVU
6725 1sUW1ELyswSVpTaFXRDCzWkdsaaEhTK2tOeWc1aDjhUjUwYjh3Wm9zQnNjSUZDa0pFbfp0UT09Ci0tLS0tRU5E
6726 IENFU1RJRK1DQVRFLS0tLS0K</crt>
6727
6728      <prv>LS0tLS1CRUdJTibBQk1WQVRFIetFWS0tLS0tCk1JSUV2Z01CQURBTkJna3Foa21HOXcwQkFRRU
6729 ZBQVNDQktnD2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M01hY1kKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4
6730 eGxiY3UyRUX6UvpJWnArc1BtQ09yaWw4SxpUS31VQTZKaGo1YwpKdnN5U1BpK1JMWitqM0h0eXVIBjdsaxGzOG
6731 JLMjZTS1Y1M0dmV1hGak1saXhxOG0vSw1oaERUNHcwdTI4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEpyV1NVWFhs
6732 c1YrRFk5cmpGMmpZNDrSE1iU1JzSwxLuh01TzVtNTA5TWCwdkEKQVdEQkQzNDg50HRAulhROVNpb1NaclREbn
6733 dKTmo3cHAwQnM4Zhh1RDbjL2poUGFWswnkem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMqzRjV25DdTcvNWRj
6734 dHZFYjZudWxxdm1HMjA5Tut1Szdwu1CukxxT2pzMTN3Zy9tT31CCmpjWWU5L314QwdNQkFBRunnZ0VCQUpRRF
6735 pxU3duMnNTUTh0SVNBTVUrvUw0zcXhrb3BzdzB4cWNScmFl0Ed4VmQKejBpOu1KbkzVQWFleTQvL3J1dndhZW1P
6736 R3RYSmZ2ai9jSny3cmJIWGIzYkjtVw9hcDhxY0RjdnhVSm1lHRUZYwQpCL3hjnvpINTlaTuFabWE1VwVQLzNjcd
6737 1zNVhhcHNpc1NXV1I4cFFZc3Z6Mmt6ci8zMXdrQxd4SGJZWHhJVDk1CjNLrmk4VTZUM1hnU1c2eFowZhp1Zn1P
6738 UzAvbXlmN5YlZVoRk1PNmFDc0x1UjZ4N1Rza2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEzdVM0bXdyR2
6739 hMz0NRY1B2MnE5V0Nia0VMNEZUzmRz1ZxchBRNG1ZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZ1F2
6740 YTbqYUgyRm5LdkExR2YxY05hGRVQ2dZRUe0NzNMUwoxcExLsmRzn2JxCmtMU3Nvt0Zhtuz1ZG1xU2ttbzh3Qj
6741 1pMXhzBElLQuD0M3U4dtdMz1ztu21ybnMwVvBtmhvRUDRyQxmzVFJocEgkU2Z4VXVsbgVGgaktjzK9xRE11TTBC
6742 OGttbFJnUFrmVHPaGnwMGVkamQwK1E5Y2V1Y25kaFp3UE16Tuc3TwRTSApKOG5yU2t5TfdMdWuXuvJNzHnbm
6743 NBRDhVYThDZ11FQXpzyjYzbzRBSH1YNjZkcEJ6TG1zYzZxS2d2ZG4xazhVcm02N3RuK2M3NkVhSEtzt1k0Rjdh
6744 S0dFSk1yeU0yQTJTe1Azdm03Rmk4eGRtblgrsx5cUx5T1VwSnZxQ012TVIKRDFpNwvftvvvoZvo20UpOK013Sm
6745 Z2RjYrK2tHa1NHOgxan0Vly21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHvtQopJZm1DW1pRSUQ1OENnWUJjamFO
6746 dk5obnFJOG9rWGHBUjR2c3NtNgPwb0tYU1ZScjRIVHo5MDFwOGdReXNCWkt0Cn1US2V6VThuUVZvTjNYWmVmBc
6747 8rVEcwYVpKOTZHky9nNTRWZmZqWTR1elVScHut3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3

```

6748 QWY5Mi9CbHZJR25FS1pMdnhLWTdVMX1Ib1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpGJNTn  
6749 VudmNUUjZxTzR0ekZtdG5TYWN3W1Ftb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU  
6750 RG1hZGsvKy9Ud2UvVk1KbmxA2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUjlhbkwzRjMKcEpUSGg4Y3FsNTdqdRRN0  
6751 FBamdyQmxrb3pOVnNMZThiWWpkcHR1MVBRs0JnQ0xDR0R1RXNBYUxwZ1RtOG44bgoyQ1h1NE52K113a1Rlczdu  
6752 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3Cc9uSVdyenRCZ1ZLC1UzSThhYnpnUUtweWrZj  
6753 VadTAXy1pZVk5TU0FIUFRHYm5jb1IzbGVPyjNLeUVXQjdsZFBHQwpOS3UwNkd5TEkKakh5TDhadEFBRXBZ1FU  
6754 OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>

6755 </cert>

6756 <revision>

6757 <time>1493650905</time>

6758 <description><! [CDATA[admin@10.97.67.135: /firewall\_rules\_edit.php made  
6759 unknown change]]></description>

6760 <username>admin@10.97.67.135</username>

6761 </revision>

6762 <gateways>

6763 <gateway\_item>

6764 <interface>lan</interface>

6765 <gateway>dynamic</gateway>

6766 <name>WAN\_DHCP</name>

6767 <weight>1</weight>

6768 <ipprotocol>inet</ipprotocol>

6769 <descr><! [CDATA[Interface WAN\_DHCP Gateway]]></descr>

6770 </gateway\_item>

6771 <gateway\_item>

6772 <interface>lan</interface>

6773 <gateway>dynamic</gateway>

6774 <name>WAN\_DHCP</name>

6775 <weight>1</weight>

6776 <ipprotocol>inet</ipprotocol>

6777 <descr><! [CDATA[Interface WAN\_DHCP Gateway]]></descr>

6778 </gateway\_item>

6779 <gateway\_item>

6780 <interface>lan</interface>

6781 <gateway>dynamic</gateway>

6782 <name>WAN\_DHCP6</name>

6783 <weight>1</weight>

6784 <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>
```

```
6819          <ipprotocol>inet</ipprotocol>
6820          <descr><! [CDATA[Gateway to VLAN 15]]></descr>
6821      </gateway_item>
6822      <gateway_item>
6823          <interface>wan</interface>
6824          <gateway>192.168.13.18</gateway>
6825          <name>GW_VLAN18</name>
6826          <weight>1</weight>
6827          <ipprotocol>inet</ipprotocol>
6828          <descr><! [CDATA[Gateway to VLAN 18]]></descr>
6829      </gateway_item>
6830      <gateway_item>
6831          <interface>wan</interface>
6832          <gateway>192.168.13.19</gateway>
6833          <name>GW_VLAN19</name>
6834          <weight>1</weight>
6835          <ipprotocol>inet</ipprotocol>
6836          <descr><! [CDATA[Gateway to VLAN 19]]></descr>
6837      </gateway_item>
6838  </gateways>
6839  <ppps/>
6840  <dyndnses/>
6841 </pfSense>
```

#### 2.10.4 Firewall Configuration for Private Cloud Subnet

```
6842 <?xml version="1.0"?>
6843 <pfSense>
6844     <version>15.4</version>
6845     <lastchange/>
6846     <theme>pfSense_ng</theme>
6847     <system>
6848         <optimization>normal</optimization>
6849         <hostname>FS-ARM</hostname>
6850         <domain>FS-ARM.gov</domain>
6851         <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/>
```

```
6887          <max_procs>2</max_procs>
6888          <nohttppreferercheck/>
6889      </webgui>
6890      <disablesegmentationoffloading/>
6891      <disablelargereceiveoffloading/>
6892      <ipv6allow/>
6893      <powerd_ac_mode>hadp</powerd_ac_mode>
6894      <powerd_battery_mode>hadp</powerd_battery_mode>
6895      <powerd_normal_mode>hadp</powerd_normal_mode>
6896      <bogons>
6897          <interval>monthly</interval>
6898      </bogons>
6899      <language>en_US</language>
6900      <dns1gw>GW_WAN</dns1gw>
6901      <dns2gw>GW_WAN</dns2gw>
6902      <dns3gw>none</dns3gw>
6903      <dns4gw>none</dns4gw>
6904      <dnsserver>10.97.74.8</dnsserver>
6905      <dnsserver>10.63.255.2</dnsserver>
6906      <maximumstates/>
6907      <aliasesresolveinterval/>
6908      <maximumtableentries/>
6909      <maximumfrags/>
6910      <enablenatreflectionpurenat>yes</enablenatreflectionpurenat>
6911      <enablebinatreflection>yes</enablebinatreflection>
6912      <enablenatreflectionhelper>yes</enablenatreflectionhelper>
6913      <reflectiontimeout/>
6914      <serialspeed>115200</serialspeed>
6915      <primaryconsole>serial</primaryconsole>
6916  </system>
6917  <interfaces>
6918      <wan>
6919          <if>em0</if>
6920          <descr><! [CDATA[WAN] ]></descr>
```

```
6921      <enable/>
6922      <spoofmac/>
6923      <ipaddr>192.168.13.20</ipaddr>
6924      <subnet>24</subnet>
6925      <gateway>GW_WAN_2</gateway>
6926      <ipaddrv6/>
6927      <subnetv6/>
6928      <gatewayv6/>
6929      </wan>
6930      <lan>
6931      <enable/>
6932      <if>em1</if>
6933      <ipaddr>192.168.20.1</ipaddr>
6934      <subnet>24</subnet>
6935      <ipaddrv6/>
6936      <subnetv6/>
6937      <media/>
6938      <mediaopt/>
6939      <track6-interface>wan</track6-interface>
6940      <track6-prefix-id>0</track6-prefix-id>
6941      <gateway/>
6942      <gatewayv6/>
6943      </lan>
6944      </interfaces>
6945      <staticroutes/>
6946      <dhcpd>
6947      <lan>
6948      <enable/>
6949      <range>
6950          <from>192.168.20.100</from>
6951          <to>192.168.20.150</to>
6952      </range>
6953      </lan>
6954      <opt1>
```

```
6955      <enable/>
6956      <range>
6957          <from>192.168.14.100</from>
6958          <to>192.168.14.150</to>
6959      </range>
6960  </opt1>
6961  <opt2>
6962      <enable/>
6963      <range>
6964          <from>192.168.15.100</from>
6965          <to>192.168.15.150</to>
6966      </range>
6967  </opt2>
6968  <opt3>
6969      <enable/>
6970      <range>
6971          <from>192.168.16.100</from>
6972          <to>192.168.16.150</to>
6973      </range>
6974  </opt3>
6975  </dhcpd>
6976  <snmpd>
6977      <syslocation/>
6978      <syscontact/>
6979      <rocommunity>public</rocommunity>
6980  </snmpd>
6981  <diag>
6982      <ipv6nat>
6983          <ipaddr/>
6984      </ipv6nat>
6985  </diag>
6986  <bridge/>
6987  <syslog/>
6988  <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>
```

```
7023             <username>admin@10.97.67.135</username>
7024         </updated>
7025     <created>
7026         <time>1493654453</time>
7027         <username>admin@10.97.67.135</username>
7028     </created>
7029 </rule>
7030 <rule>
7031     <id/>
7032     <tracker>1493654529</tracker>
7033     <type>pass</type>
7034     <interface>wan</interface>
7035     <ipprotocol>inet</ipprotocol>
7036     <tag/>
7037     <tagged/>
7038     <direction>any</direction>
7039     <quick>yes</quick>
7040     <floating>yes</floating>
7041     <max/>
7042     <max-src-nodes/>
7043     <max-src-conn/>
7044     <max-src-states/>
7045     <statetimeout/>
7046     <statetype>keep state</statetype>
7047     <os/>
7048     <protocol>tcp</protocol>
7049     <source>
7050         <any/>
7051     </source>
7052     <destination>
7053         <network>lan</network>
7054         <port>80</port>
7055     </destination>
7056     <descr><![CDATA[Allow HTTP connection to LAN server]]></descr>
```

```
7057      <updated>
7058          <time>1493654529</time>
7059          <username>admin@10.97.67.135</username>
7060      </updated>
7061      <created>
7062          <time>1493654529</time>
7063          <username>admin@10.97.67.135</username>
7064      </created>
7065  </rule>
7066  <rule>
7067      <id/>
7068      <tracker>1493654337</tracker>
7069      <type>pass</type>
7070      <interface>wan</interface>
7071      <ipprotocol>inet</ipprotocol>
7072      <tag/>
7073      <tagged/>
7074      <direction>any</direction>
7075      <quick>yes</quick>
7076      <floating>yes</floating>
7077      <max/>
7078      <max-src-nodes/>
7079      <max-src-conn/>
7080      <max-src-states/>
7081      <statetimeout/>
7082      <statetype>keep state</statetype>
7083      <os/>
7084      <protocol>tcp</protocol>
7085      <source>
7086          <any/>
7087      </source>
7088      <destination>
7089          <network>lan</network>
7090          <port>3389</port>
```

```
7091             </destination>
7092             <descr><! [CDATA[Allow RDP Connection to LAN servers]]></descr>
7093             <created>
7094                 <time>1493654337</time>
7095                 <username>admin@10.97.67.135</username>
7096             </created>
7097             <updated>
7098                 <time>1493654474</time>
7099                 <username>admin@10.97.67.135</username>
7100             </updated>
7101         </rule>
7102         <rule>
7103             <id/>
7104             <tracker>1469131237</tracker>
7105             <type>pass</type>
7106             <interface>wan</interface>
7107             <ipprotocol>inet</ipprotocol>
7108             <tag/>
7109             <tagged/>
7110             <max/>
7111             <max-src-nodes/>
7112             <max-src-conn/>
7113             <max-src-states/>
7114             <statetimeout/>
7115             <statetype>keep state</statetype>
7116             <os/>
7117             <protocol>tcp</protocol>
7118             <source>
7119                 <any/>
7120             </source>
7121             <destination>
7122                 <network>wanip</network>
7123                 <port>80</port>
7124             </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>
```

```
7159          <time>1465935224</time>
7160          <username>admin@192.168.18.100</username>
7161        </updated>
7162        <created>
7163          <time>1465935224</time>
7164          <username>admin@192.168.18.100</username>
7165        </created>
7166      </rule>
7167      <rule>
7168        <id/>
7169        <tracker>1461788221</tracker>
7170        <type>pass</type>
7171        <interface>wan</interface>
7172        <ipprotocol>inet</ipprotocol>
7173        <tag/>
7174        <tagged/>
7175        <max/>
7176        <max-src-nodes/>
7177        <max-src-conn/>
7178        <max-src-states/>
7179        <statetimeout/>
7180        <statetype>keep state</statetype>
7181        <os/>
7182        <protocol>tcp</protocol>
7183        <source>
7184          <any/>
7185        </source>
7186        <destination>
7187          <network>wanip</network>
7188          <port>443</port>
7189        </destination>
7190        <descr><! [CDATA[Allow Port 443 on WAN]]></descr>
7191        <created>
7192          <time>1461788221</time>
```

```
7193                  <username>admin@192.168.1.2</username>
7194          </created>
7195          <updated>
7196              <time>1493654159</time>
7197          <username>admin@10.97.67.135</username>
7198      </updated>
7199  </rule>
7200  <rule>
7201      <id/>
7202      <tracker>1468437174</tracker>
7203      <type>pass</type>
7204      <interface>lan</interface>
7205      <ipprotocol>inet</ipprotocol>
7206      <tag/>
7207      <tagged/>
7208      <max/>
7209      <max-src-nodes/>
7210      <max-src-conn/>
7211      <max-src-states/>
7212      <statetimeout/>
7213      <statetype>keep state</statetype>
7214      <os/>
7215      <protocol>tcp/udp</protocol>
7216      <source>
7217          <any/>
7218      </source>
7219      <destination>
7220          <any/>
7221      </destination>
7222      <descr/>
7223      <updated>
7224          <time>1468437174</time>
7225          <username>admin@192.168.20.100</username>
7226      </updated>
```

```
7227          <created>
7228              <time>1468437174</time>
7229              <username>admin@192.168.20.100</username>
7230          </created>
7231          <disabled/>
7232      </rule>
7233      <rule>
7234          <id/>
7235          <tracker>1465935241</tracker>
7236          <type>pass</type>
7237          <interface>lan</interface>
7238          <ipprotocol>inet</ipprotocol>
7239          <tag/>
7240          <tagged/>
7241          <max/>
7242          <max-src-nodes/>
7243          <max-src-conn/>
7244          <max-src-states/>
7245          <statetimeout/>
7246          <statetype>keep state</statetype>
7247          <os/>
7248          <protocol>icmp</protocol>
7249          <source>
7250              <any/>
7251          </source>
7252          <destination>
7253              <any/>
7254          </destination>
7255          <descr/>
7256          <updated>
7257              <time>1465935241</time>
7258              <username>admin@192.168.18.100</username>
7259          </updated>
7260          <created>
```

```
7261          <time>1465935241</time>
7262          <username>admin@192.168.18.100</username>
7263      </created>
7264  </rule>
7265  <rule>
7266      <type>pass</type>
7267      <ipprotocol>inet</ipprotocol>
7268      <descr><! [CDATA[Default allow LAN to any rule] ]></descr>
7269      <interface>lan</interface>
7270      <tracker>0100000101</tracker>
7271      <source>
7272          <network>lan</network>
7273      </source>
7274      <destination>
7275          <any/>
7276      </destination>
7277  </rule>
7278  <rule>
7279      <type>pass</type>
7280      <ipprotocol>inet6</ipprotocol>
7281      <descr><! [CDATA[Default allow LAN IPv6 to any rule] ]></descr>
7282      <interface>lan</interface>
7283      <tracker>0100000102</tracker>
7284      <source>
7285          <network>lan</network>
7286      </source>
7287      <destination>
7288          <any/>
7289      </destination>
7290  </rule>
7291  <separator>
7292      <wan/>
7293      <lan/>
7294      <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>
```

```
7328          <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
7329 sshlockout</command>
7330      </item>
7331      <item>
7332          <minute>*/60</minute>
7333          <hour>*</hour>
7334          <mday>*</mday>
7335          <month>*</month>
7336          <wday>*</wday>
7337          <who>root</who>
7338          <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
7339 webConfiguratorlockout</command>
7340      </item>
7341      <item>
7342          <minute>1</minute>
7343          <hour>1</hour>
7344          <mday>*</mday>
7345          <month>*</month>
7346          <wday>*</wday>
7347          <who>root</who>
7348          <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
7349      </item>
7350      <item>
7351          <minute>*/60</minute>
7352          <hour>*</hour>
7353          <mday>*</mday>
7354          <month>*</month>
7355          <wday>*</wday>
7356          <who>root</who>
7357          <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
7358 virusprot</command>
7359      </item>
7360      <item>
7361          <minute>30</minute>
7362          <hour>12</hour>
```

```
7363      <mday>*</mday>
7364      <month>*</month>
7365      <wday>*</wday>
7366      <who>root</who>
7367      <command>/usr/bin/nice -n20 /etc/rc.update_urllables</command>
7368      </item>
7369      </cron>
7370      <wol/>
7371      <rrd>
7372          <enable/>
7373      </rrd>
7374      <load_balancer>
7375          <monitor_type>
7376              <name>ICMP</name>
7377              <type>icmp</type>
7378              <descr><! [CDATA[ ICMP ]]></descr>
7379              <options/>
7380          </monitor_type>
7381          <monitor_type>
7382              <name>TCP</name>
7383              <type>tcp</type>
7384              <descr><! [CDATA[ Generic TCP ]]></descr>
7385              <options/>
7386          </monitor_type>
7387          <monitor_type>
7388              <name>HTTP</name>
7389              <type>http</type>
7390              <descr><! [CDATA[ Generic HTTP ]]></descr>
7391              <options>
7392                  <path></path>
7393                  <host/>
7394                  <code>200</code>
7395              </options>
7396          </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      <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
7419 /sequence>
7420
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/>
```

```

7432          <dnssecstripped/>
7433          <domainoverrides>
7434              <domain>acmefinancial.com</domain>
7435              <ip>192.168.19.10</ip>
7436              <descr><! [CDATA[Active Directory]]></descr>
7437          </domainoverrides>
7438          <port/>
7439          <system_domain_local_zone_type>transparent</system_domain_local_zone_type>
7440          <enable/>
7441          </unbound>
7442          <dhcpdv6>
7443              <lan>
7444                  <range>
7445                      <from>::1000</from>
7446                      <to>::2000</to>
7447                  </range>
7448                  <ramode>assist</ramode>
7449                  <rapriority>medium</rapriority>
7450              </lan>
7451          </dhcpdv6>
7452          <cert>
7453              <refid>5720a0502b277</refid>
7454              <descr><! [CDATA[webConfigurator default (5720a0502b277) ]]></descr>
7455              <type>server</type>
7456          <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCK1JSUZiVENDQkZXZ0F3SUJBZ01CQURBTkJna3
7457 Foa2lHOXcwQkFRc0ZBRENcDcERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnT1ZCQWduQ1ZOMF1YUmxFNUkV3RHdZ
7458 RFZRUUhFd2hNYjJOaGJHbDB1VEU0TURzR0ExVUVDaE12Y0daVApaVzV6W1NCM1pXSkRiMjVtYVdkMWNTRjBiM0
7459 lnVTJWc1ppMVRhV2R1W1dRZ1EyVn1kR2xtYVdOaGRHVxhLREFtCkJna3Foa2lHOXcwQkNRRVdHV0ZrYldsdfVFI
7460 Qm1VMlZ1YzJvdWJHowPZV3hrYjIxAGFXNHhIakFjQmdOVkJBTvQKRlhCbVUyVnVjM1V0T1RjeU1HRXdOVEF5WW
7461 pJM056QWVGdzB4TmpBME1qY3hNVEU1TkrSYUZ3MH1NVEV3TVRneApNVEU1TkrSYU1JRzBNuXN3Q1FZRFZRUUdF
7462 d0pWVXpFT01Bd0dBMVVFQ0JNR1UzUmhkR1V4RVRBUEJnT1ZCQWNNUckNFeHZMkZzYVhSNU1UZ3dOZ11EV1FRS0
7463 V5OXdabE5sYm5ObElIZGxza052YmlacFozVn1ZWfJ2Y21CVFpXeG0KTFZoCfoyNWxaQ0JEWlhKMGFxWnBZMkYw
7464 W1Rfb01DWUDuDU3FHU01iM0RRRUpBU1laWVdSdGFXNUFjR1pUW1c1egpaUzVzYjJOAGJHUnZiV0ZwYmpFZU1Cd0
7465 dBMVVFQXhNvmNHW1RaVzV6W1MwMU56SXdZVEEXtURKaU1qYzNNSU1CCk1qQU5CZ2txaGtpRz13MEJBuuVGQUFP
7466 Q0FROEFNSU1CQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFmUE1aVzNMdG
7467 hDODBH0dhZnJENWdqctrwZkNNMh1zbEFFPaV1ZK1hDYjdNa20dmtTMgpmbz14emNyaDiUrNV1aY1BHeXR1a2ls
7468 ZWR4bjFWeF16S11zYXZKdn1Kb11RMctNTkx0dkFjYnRhTUFoZjh1ZkRFC1hrc1NVQ0N5YTFrbEYxNWJGZmcyUG
7469 E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkuFRJTkx3QUZnd1E5K1BQZkwKVTQxMFbVb3FFbWEwdzU4Q1RZKzZh
7470 ZEFiUEhjWGc5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxFmdCUApyeXd1SEZwd3J1LytyWExieEcrcD
7471 dwYXI0aHR0UFRDcm11NmFqQVVTNmpvN05kOE1QNWPzZ1kzR0h2ZjhzUU1ECKfrQUJvNE1CaGpDQ0FZSXdDUV1E
7472 V1IwVEJBSxdBREFSQmdsZ2hrZ0JdmhDQVFFRUJBTUNCa0F3TxDzS11JWkkKQV1iNFFnRu5CQ11XSkU5d1pXNV
7473
7474

```

7475 RVMHdnUjJWdVpYSmhkR1ZrSUZObGNuWmxjaUJEWlhKMGFXWnBZMkYwW1RBZApCZ05WSFE0RUZnUVU3K11LRmNp  
 7476 OFFVSGhTZ0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K11LCkZjaThRVUhoU2dMRHY4RUNzY0  
 7477 Nkd0FLaGdicWtnYmN3Z2JReEN6QuPcZ05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex  
 7478 VUVCeE1JVec5allXeHBkSGt4T0RBMkJnT1ZCQW9UTDNCbVUyVnVjM1VnZDJWaQpRMj11Wm1sbmRYSmhkRz15SU  
 7479 ZobGJHWXRVMmxuYm1Wa01FTmxjb1JwWm1sa11YUmxBu2d3SmdZSktvWk1odmNOCKFRa0JGaGxoWkcxcGJrQnda  
 7480 bE5sYm5ObExteHZZMkzzWkc5dF1XbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU  
 7481 56ZUNBUUF3SFFZRFZSMGxCQ113RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd01G  
 7482 b0RBTkJna3Foa21HOXcwQkFRc0ZBQU9DQVFFQXJxFpQdXd2MVzuUC82NmJDWFJ5CkVmaW1LRW1PcmtNaTB5M0  
 7483 9PWGtzWEs1cEM2dTd6Uk13WjEvRjYyRUp3OD1UOWx4Y01ZelZOTm5Idlg0bXFPRUckUWJhRU42NEkxOHFud3Zm  
 7484 S2JrREZvRThMR1hSdzBkMnAyTGVmYTd4YTIVSGNHc0xHTktPbkJxb3N4ejurQ1B3ZwpWeVRaTS9wV3p3aDdQRG  
 7485 c4bGdrcVc3dSt1b01DNDJ1bVjkOURCTmlzdFJ4Rv1NmKfLQkFsZG1LYStvRUY1VUuwCm43aXpvN1Z4dHJWMTJv  
 7486 TTdyS11RQ05kY00xZkVsEuwvb3ZkUnVpa0F5Wm1VvnFUL1dDZGo3dDdIVG9ob0RFYzEKSklkOvpPSmR2QmZLVU  
 7487 1suW1ELyswSVpTaFXRdczWkdsaaEhTK2t0ewc1aDjhUjUwYjh3Wm9zQnjSUZDa0pFbgp0UT09Ci0tLS0tRU5E  
 7488 IENFU1RJRk1DQVRFLS0tLS0K</crt>  
 7489  
 7490 <prv>LS0tLS1CRUDJTibQuk1WQVRFIETFWS0tLS0tck1JSUV2Z01CQURBTkJna3Foa21HOXcwQkFRRU  
 7491 ZBQVNDQktn2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M01hY1kKMjN3YkNKR1htWFJWKy9odVVKeFdsc3hxb3M4  
 7492 eGxiY3UyRUX6UvpJWnArc1BtQ09yaWw4SXpUS31VQTZKaGo1YwpKdnN5U1BpK1JMWitqM0h0eXVIbjdsaxGxzOG  
 7493 JLMjZTS1Y1M0dmV1hGak1saXhxOG0vSW1oaERUNHcwdTI4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEpyV1NVWFhs  
 7494 c1YrRFk5cmpGMmpZNDdrSE1iU1JZSWxLUHo1TzVtNTA5TWcwdkEKQVdEQkQzNDg5OHRUalhROVNpb1NaclREbn  
 7495 dKTmo3cHAwQnM4Zhh1RDBjL2pouGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj  
 7496 dHZFYjZudWxxdm1HMjA5TUt1Szdwu1CukxxT2pzMTN3Zy9tT31CCmpjWWU5L314QWdNQkFBRunnz0VCQUpRRF  
 7497 pxU3duMnNTUTH0SVNBTVUrUW0zcXhrb3Bzdzb4cWNScmFl0Ed4VmQKejBpOU1KbkZVQWFleTQvL3J1ndnhZW1P  
 7498 R3RYSmZ2ai9jSny3cmJIWGIzYkjtVW9hcDhxY0RjdVSMmlHRUZYWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcd  
 7499 1zNVhhcHNpc1NXV1I4cffZc3Z6Mmt6ci8zMXdrQxd4SGJZWHhJVDk1CjNLrmk4VTZUM1hnU1c2eFowZhp1ZnlP  
 7500 UzAvbXlmNU5YLzVoRk1PNmFDc0x1UjZ4N1Rza2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEzdVM0bXdyR2  
 7501 hMz0NRY1B2MnE5V0Nia0VMNEZUZmRz1ZXchBRNG1ZVWtwNzhMY1FPMPgpsSGR5cTJxTmjsNDIwa3h5M2FnZ1F2  
 7502 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUE0NzNMUwoxcExLSmRZN2JxCmtMU3NVT0zHTUZ1ZG1xU2ttbzh3Qj  
 7503 1pMXhzBElLQuD0M3U4dTdMz1TzU21ybnMwVVTMHRVUDRyQXmzVFJocEgKU2Z4VXVsbGVGaktjzK9xRE11TTBC  
 7504 OGttbFJnUFRmVHPaGNwMGVkamQwK1E5Y2V1Y25kaFp3UE16Tuc3TWRTSApKOG5yU2t5TfdMdWUxUVJNZHnbm  
 7505 NBRDhVYThDZ11FQXpzyjYzbzRBSH1YNjZkcEJ6TG1zYzZxS2d2ZG4xazhVcm02N3RuK2M3NkVhSEtZT1k0Rjdh  
 7506 S0dFSk1yeU0yQTJTe1Azdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZQ012TVIKRDFpNWVFTVvoZvo20UpOK013Sm  
 7507 Z2RjYrK2tHa1NHOGxa0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDnsTHvtQOpJZm1DWlPRSUQ1OENnWUJjamFO  
 7508 dk5obnFJOG9rWGhBUjR2c3NtNgPwb0tYU1ZScjRIVh05MDfwOGdReXNCWkt0Cn1US2V6VThuUVZvTjNYWmVmBc  
 7509 8rVEcwYVpKOTZHky9nNTRWZmZqWTR1elVScHhut3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3  
 7510 QWY5Mi9CbHZJR25FS1pMdnhLWTdVmx1Ib1NRLzczUG1DSnfqemd6UUtCZ1FDZgpJQje3RzRnWWNGL3hpDGJNTn  
 7511 VudmNUUjZxTzR0ekTzdG5TYWN3W1Ftb2UvdUVIaGE0bU84WTBCeTNRcitvU1BCCndVR2RiUnNhdTgxcU12VutU  
 7512 RG1hZGsvKy9Ud2UvVk1Kbm2x2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUj1hbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0  
 7513 FBamdyQmxrb3pOVnNMZThiWWpkcHR1MVBRs0JnQ0xDR0R1RXNBYUxwZ1RtOG44bgoyQ1h1NE52K113a1Rlczdu  
 7514 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFevSDgxMHRGd1p3cc9uSVDycnRCZ1ZLClUzSThhYnpnUUtOewrZj  
 7515 VadTAxY1pZVk5TU0FIUFRHym5j1b1IzbGPVYjNLeUVXQjdsZFBHQwpOS3UwNkd5TEkKakh5TDhadEFBRXBZ1FU  
 7516 OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>

7517 </cert>

7518 <revision>

7519 <time>1493654529</time>

7520 <description><![CDATA[admin@10.97.67.135: /firewall\_rules\_edit.php made  
 7521 unknown change]]></description>

7522 <username>admin@10.97.67.135</username>

7523 </revision>

7524 <gateways>

7525 <gateway\_item>

7526 <interface>wan</interface>

```
7527      <gateway>192.168.13.1</gateway>
7528      <name>GW_WAN_2</name>
7529      <weight>1</weight>
7530      <ipprotocol>inet</ipprotocol>
7531      <interval/>
7532      <descr><! [CDATA[Interface wan Gateway] ]></descr>
7533      </gateway_item>
7534    </gateways>
7535    <ppps/>
7536    <dyndnses/>
7537    <dnsmasq>
7538      <enable/>
7539      <custom_options/>
7540      <port>53</port>
7541      <interface/>
7542      <hosts>
7543        <host>activedirectory</host>
7544        <domain>acmefinancial.com</domain>
7545        <ip>192.168.19.10</ip>
7546        <descr/>
7547        <aliases/>
7548      </hosts>
7549    </dnsmasq>
7550  </pfSense>
```

## 2.10.5 Firewall Configuration for the Management and Monitoring Subnet

```
7551  <?xml version="1.0"?>
7552
7553  <pfSense>
7554    <version>15.4</version>
7555    <lastchange/>
7556    <theme>pfSense_ng</theme>
7557    <system>
7558      <optimization>normal</optimization>
7559      <hostname>FS-ARM</hostname>
7560      <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>
```

```
7595          <port/>
7596          <max_procs>2</max_procs>
7597          <nohttppreferercheck/>
7598      </webgui>
7599      <disablenatreflection>yes</disablenatreflection>
7600      <disablesegmentationoffloading/>
7601      <disablelargereceiveoffloading/>
7602      <ipv6allow/>
7603      <powerd_ac_mode>hadp</powerd_ac_mode>
7604      <powerd_battery_mode>hadp</powerd_battery_mode>
7605      <powerd_normal_mode>hadp</powerd_normal_mode>
7606      <bogons>
7607          <interval>monthly</interval>
7608      </bogons>
7609      <language>en_US</language>
7610      <dns1gw>GW_WAN</dns1gw>
7611      <dns2gw>GW_WAN</dns2gw>
7612      <dns3gw>none</dns3gw>
7613      <dns4gw>none</dns4gw>
7614      <dnsserver>10.97.74.8</dnsserver>
7615      <dnsserver>10.63.255.2</dnsserver>
7616      <serialspeed>115200</serialspeed>
7617      <primaryconsole>serial</primaryconsole>
7618      <maximumstates/>
7619      <aliasesresolveinterval/>
7620      <maximumtableentries/>
7621      <maximumfrags/>
7622      <reflectiontimeout/>
7623  </system>
7624  <interfaces>
7625      <wan>
7626          <if>em0</if>
7627          <descr><! [CDATA[WAN] ]></descr>
7628          <enable/>
```

```
7629      <spoofmac/>
7630      <ipaddr>192.168.13.17</ipaddr>
7631      <subnet>24</subnet>
7632      <gateway>GW_WAN_2</gateway>
7633      <ipaddrv6/>
7634      <subnetv6/>
7635      <gatewayv6/>
7636      </wan>
7637      <lan>
7638          <enable/>
7639          <if>em1</if>
7640          <ipaddr>192.168.17.1</ipaddr>
7641          <subnet>24</subnet>
7642          <ipaddrv6/>
7643          <subnetv6/>
7644          <media/>
7645          <mediaopt/>
7646          <track6-interface>wan</track6-interface>
7647          <track6-prefix-id>0</track6-prefix-id>
7648          <gateway/>
7649          <gatewayv6/>
7650      </lan>
7651  </interfaces>
7652  <staticroutes>
7653      <route>
7654          <network>192.168.19.0/24</network>
7655          <gateway>GW_VLAN19</gateway>
7656          <descr><! [CDATA[Route to VLAN 2019]]></descr>
7657      </route>
7658  </staticroutes>
7659  <dhcpd>
7660      <lan>
7661          <enable/>
7662          <range>
```

```
7663          <from>192.168.17.100</from>
7664          <to>192.168.17.150</to>
7665          </range>
7666          </lan>
7667          <opt1>
7668          <enable/>
7669          <range>
7670          <from>192.168.14.100</from>
7671          <to>192.168.14.150</to>
7672          </range>
7673          </opt1>
7674          <opt2>
7675          <enable/>
7676          <range>
7677          <from>192.168.15.100</from>
7678          <to>192.168.15.150</to>
7679          </range>
7680          </opt2>
7681          <opt3>
7682          <enable/>
7683          <range>
7684          <from>192.168.16.100</from>
7685          <to>192.168.16.150</to>
7686          </range>
7687          </opt3>
7688          </dhcpd>
7689          <snmpd>
7690          <syslocation/>
7691          <syscontact/>
7692          <rocommunity>public</rocommunity>
7693          </snmpd>
7694          <diag>
7695          <ipv6nat>
7696          <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/>
```

```
7731      </nat>
7732      <filter>
7733          <rule>
7734              <id/>
7735              <tracker>1493655499</tracker>
7736              <type>pass</type>
7737              <interface>wan</interface>
7738              <ipprotocol>inet</ipprotocol>
7739              <tag/>
7740              <tagged/>
7741              <direction>any</direction>
7742              <quick>yes</quick>
7743              <floating>yes</floating>
7744              <max/>
7745              <max-src-nodes/>
7746              <max-src-conn/>
7747              <max-src-states/>
7748              <statetimeout/>
7749              <statetype>keep state</statetype>
7750              <os></os>
7751              <protocol>tcp/udp</protocol>
7752          <source>
7753              <any/>
7754          </source>
7755          <destination>
7756              <network>lan</network>
7757              <port>514</port>
7758          </destination>
7759          <descr><![CDATA[Allow Connection to syslog in LAN]]></descr>
7760          <updated>
7761              <time>1493655499</time>
7762              <username>admin@10.97.67.135</username>
7763          </updated>
7764          <created>
```

```
7765          <time>1493655499</time>
7766          <username>admin@10.97.67.135</username>
7767        </created>
7768      </rule>
7769    <rule>
7770      <id/>
7771      <tracker>1493649494</tracker>
7772      <type>pass</type>
7773      <interface>wan</interface>
7774      <ipprotocol>inet</ipprotocol>
7775      <tag/>
7776      <tagged/>
7777      <direction>any</direction>
7778      <quick>yes</quick>
7779      <floating>yes</floating>
7780      <max/>
7781      <max-src-nodes/>
7782      <max-src-conn/>
7783      <max-src-states/>
7784      <statetimeout/>
7785      <statetype>keep state</statetype>
7786      <os/>
7787      <protocol>tcp</protocol>
7788      <source>
7789        <any/>
7790      </source>
7791      <destination>
7792        <network>lan</network>
7793        <port>1433-1434</port>
7794      </destination>
7795      <descr><! [CDATA[Allow Connection to Sharepoint database-1433 and
7796 143] ]></descr>
7797      <created>
7798        <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>
```

```
7833      <updated>
7834          <time>1493649686</time>
7835          <username>admin@10.97.67.135</username>
7836      </updated>
7837      <created>
7838          <time>1493649686</time>
7839          <username>admin@10.97.67.135</username>
7840      </created>
7841  </rule>
7842  <rule>
7843      <id/>
7844      <tracker>1493649754</tracker>
7845      <type>pass</type>
7846      <interface>wan</interface>
7847      <ipprotocol>inet</ipprotocol>
7848      <tag/>
7849      <tagged/>
7850      <direction>any</direction>
7851      <quick>yes</quick>
7852      <floating>yes</floating>
7853      <max/>
7854      <max-src-nodes/>
7855      <max-src-conn/>
7856      <max-src-states/>
7857      <statetimeout/>
7858      <statetype>keep state</statetype>
7859      <os/>
7860      <protocol>tcp</protocol>
7861      <source>
7862          <any/>
7863      </source>
7864      <destination>
7865          <network>lan</network>
7866          <port>389</port>
```

```
7867          </destination>
7868          <descr><! [CDATA[Allow LDAP Connection to LAN]]></descr>
7869          <created>
7870              <time>1493649754</time>
7871              <username>admin@10.97.67.135</username>
7872          </created>
7873          <updated>
7874              <time>1493650257</time>
7875              <username>admin@10.97.67.135</username>
7876          </updated>
7877      </rule>
7878      <rule>
7879          <id/>
7880          <tracker>1493650231</tracker>
7881          <type>pass</type>
7882          <interface>wan</interface>
7883          <ipprotocol>inet</ipprotocol>
7884          <tag/>
7885          <tagged/>
7886          <direction>any</direction>
7887          <quick>yes</quick>
7888          <floating>yes</floating>
7889          <max/>
7890          <max-src-nodes/>
7891          <max-src-conn/>
7892          <max-src-states/>
7893          <statetimeout/>
7894          <statetype>keep state</statetype>
7895          <os/>
7896          <protocol>tcp</protocol>
7897          <source>
7898              <any/>
7899          </source>
7900          <destination>
```

```
7901             <network>lan</network>
7902                 <port>2389</port>
7903             </destination>
7904         <descr><! [CDATA[Allow Alternate LDAP Connection to Radiant
7905     ]]></descr>
7906             <updated>
7907                 <time>1493650231</time>
7908                 <username>admin@10.97.67.135</username>
7909             </updated>
7910             <created>
7911                 <time>1493650231</time>
7912                 <username>admin@10.97.67.135</username>
7913             </created>
7914         </rule>
7915         <rule>
7916             <id/>
7917             <tracker>1493649801</tracker>
7918             <type>pass</type>
7919             <interface>wan</interface>
7920             <ipprotocol>inet</ipprotocol>
7921             <tag/>
7922             <tagged/>
7923             <direction>any</direction>
7924             <quick>yes</quick>
7925             <floating>yes</floating>
7926             <max/>
7927             <max-src-nodes/>
7928             <max-src-conn/>
7929             <max-src-states/>
7930             <statetimeout/>
7931             <statetype>keep state</statetype>
7932             <os/>
7933             <protocol>tcp</protocol>
7934             <source>
```

```
7935          <any/>
7936      </source>
7937      <destination>
7938          <network>lan</network>
7939          <port>636</port>
7940      </destination>
7941      <descr><! [CDATA[Allow LDAPS Connection to LAN] ]></descr>
7942      <created>
7943          <time>1493649801</time>
7944          <username>admin@10.97.67.135</username>
7945      </created>
7946      <updated>
7947          <time>1493650283</time>
7948          <username>admin@10.97.67.135</username>
7949      </updated>
7950  </rule>
7951  <rule>
7952      <id/>
7953      <tracker>1493649895</tracker>
7954      <type>pass</type>
7955      <interface>wan</interface>
7956      <ipprotocol>inet</ipprotocol>
7957      <tag/>
7958      <tagged/>
7959      <direction>any</direction>
7960      <quick>yes</quick>
7961      <floating>yes</floating>
7962      <max/>
7963      <max-src-nodes/>
7964      <max-src-conn/>
7965      <max-src-states/>
7966      <statetimeout/>
7967      <statetype>keep state</statetype>
7968      <os/>
```

```
7969          <protocol>tcp</protocol>
7970          <source>
7971              <any/>
7972          </source>
7973          <destination>
7974              <network>lan</network>
7975              <port>8000</port>
7976          </destination>
7977          <descr><![CDATA[Allow Connection to Port 8000 -Splunk
7978 Web]]></descr>
7979          <created>
7980              <time>1493649895</time>
7981              <username>admin@10.97.67.135</username>
7982          </created>
7983          <updated>
7984              <time>1493649933</time>
7985              <username>admin@10.97.67.135</username>
7986          </updated>
7987      </rule>
7988      <rule>
7989          <id/>
7990          <tracker>1493650131</tracker>
7991          <type>pass</type>
7992          <interface>wan</interface>
7993          <ipprotocol>inet</ipprotocol>
7994          <tag/>
7995          <tagged/>
7996          <direction>any</direction>
7997          <quick>yes</quick>
7998          <floating>yes</floating>
7999          <max/>
8000          <max-src-nodes/>
8001          <max-src-conn/>
8002          <max-src-states/>
```

```
8003          <statetimeout/>
8004          <statetype>keep state</statetype>
8005          <os/>
8006          <protocol>tcp</protocol>
8007          <source>
8008              <any/>
8009          </source>
8010          <destination>
8011              <network>lan</network>
8012              <port>8089</port>
8013          </destination>
8014          <descr><! [CDATA[Allow Connection to Port 8089 -Splunk management
8015 por]]></descr>
8016          <updated>
8017              <time>1493650131</time>
8018              <username>admin@10.97.67.135</username>
8019          </updated>
8020          <created>
8021              <time>1493650131</time>
8022              <username>admin@10.97.67.135</username>
8023          </created>
8024      </rule>
8025      <rule>
8026          <id/>
8027          <tracker>1493650643</tracker>
8028          <type>pass</type>
8029          <interface>wan</interface>
8030          <ipprotocol>inet</ipprotocol>
8031          <tag/>
8032          <tagged/>
8033          <direction>any</direction>
8034          <quick>yes</quick>
8035          <floating>yes</floating>
8036          <max/>
```

```
8037          <max-src-nodes/>
8038          <max-src-conn/>
8039          <max-src-states/>
8040          <statetimeout/>
8041          <statetype>keep state</statetype>
8042          <os/>
8043          <protocol>tcp</protocol>
8044          <source>
8045              <any/>
8046          </source>
8047          <destination>
8048              <network>lan</network>
8049              <port>9997</port>
8050          </destination>
8051          <descr><! [CDATA[Allow Connection to Port 9997 -Splunk
8052 Forwarding]]></descr>
8053          <updated>
8054              <time>1493650643</time>
8055              <username>admin@10.97.67.135</username>
8056          </updated>
8057          <created>
8058              <time>1493650643</time>
8059              <username>admin@10.97.67.135</username>
8060          </created>
8061      </rule>
8062      <rule>
8063          <id/>
8064          <tracker>1481037634</tracker>
8065          <type>pass</type>
8066          <interface>lan</interface>
8067          <ipprotocol>inet</ipprotocol>
8068          <tag/>
8069          <tagged/>
8070          <direction>any</direction>
```

```
8071          <quick>yes</quick>
8072          <floating>yes</floating>
8073          <max/>
8074          <max-src-nodes/>
8075          <max-src-conn/>
8076          <max-src-states/>
8077          <statetimeout/>
8078          <statetype>keep state</statetype>
8079          <os/>
8080          <source>
8081              <address>192.168.17.100</address>
8082          </source>
8083          <destination>
8084              <any/>
8085          </destination>
8086          <descr><! [CDATA[Allow Radiant (192.168.17.100) to outside -
8087 LAN] ]></descr>
8088          <created>
8089              <time>1481037634</time>
8090              <username>admin@10.97.67.155</username>
8091          </created>
8092          <updated>
8093              <time>1481037861</time>
8094              <username>admin@10.97.67.155</username>
8095          </updated>
8096          <disabled/>
8097      </rule>
8098      <rule>
8099          <id/>
8100          <tracker>1481037754</tracker>
8101          <type>pass</type>
8102          <interface>wan</interface>
8103          <ipprotocol>inet</ipprotocol>
8104          <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>
```

```
8173      <type>pass</type>
8174      <interface>wan</interface>
8175      <ipprotocol>inet</ipprotocol>
8176      <tag/>
8177      <tagged/>
8178      <max/>
8179      <max-src-nodes/>
8180      <max-src-conn/>
8181      <max-src-states/>
8182      <statetimeout/>
8183      <statetype>keep state</statetype>
8184      <os/>
8185      <protocol>tcp/udp</protocol>
8186      <source>
8187          <any/>
8188      </source>
8189      <destination>
8190          <network>wanip</network>
8191          <port>80</port>
8192      </destination>
8193      <descr><! [CDATA[Allow to Port 80 on Firewall WAN] ]></descr>
8194      <created>
8195          <time>1469130242</time>
8196          <username>admin@192.168.17.103</username>
8197      </created>
8198      <updated>
8199          <time>1493649052</time>
8200          <username>admin@10.97.67.135</username>
8201      </updated>
8202      </rule>
8203      <rule>
8204          <id/>
8205          <tracker>1465935549</tracker>
8206          <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>
```

```
8241          <tag/>
8242          <tagged/>
8243          <max/>
8244          <max-src-nodes/>
8245          <max-src-conn/>
8246          <max-src-states/>
8247          <statetimeout/>
8248          <statetype>keep state</statetype>
8249          <os/>
8250          <protocol>tcp</protocol>
8251          <source>
8252          <any/>
8253          </source>
8254          <destination>
8255          <network>wanip</network>
8256          <port>443</port>
8257          </destination>
8258          <descr><! [CDATA[Allow to Port 443 on Firewall WAN] ]></descr>
8259          <created>
8260          <time>1461788221</time>
8261          <username>admin@192.168.1.2</username>
8262          </created>
8263          <updated>
8264          <time>1493649121</time>
8265          <username>admin@10.97.67.135</username>
8266          </updated>
8267          </rule>
8268          <rule>
8269          <source>
8270          <any/>
8271          </source>
8272          <interface>wan</interface>
8273          <protocol>tcp/udp</protocol>
8274          <destination>
```

```
8275             <address>192.168.17.11</address>
8276                 <port>5176</port>
8277             </destination>
8278             <descr><![CDATA[NAT Mapping to ConsoleWorks]]></descr>
8279             <associated-rule-id>nat_57bf06b1aa4c21.26556306</associated-rule-
8280         id>
8281             <tracker>1472136881</tracker>
8282             <created>
8283                 <time>1472136881</time>
8284                 <username>NAT Port Forward</username>
8285             </created>
8286             <disabled/>
8287         </rule>
8288         <rule>
8289             <id/>
8290             <tracker>1469130278</tracker>
8291             <type>pass</type>
8292             <interface>lan</interface>
8293             <ipprotocol>inet</ipprotocol>
8294             <tag/>
8295             <tagged/>
8296             <max/>
8297             <max-src-nodes/>
8298             <max-src-conn/>
8299             <max-src-states/>
8300             <statetimeout/>
8301             <statetype>keep state</statetype>
8302             <os/>
8303             <protocol>tcp/udp</protocol>
8304             <source>
8305                 <any/>
8306             </source>
8307             <destination>
8308                 <any/>
```

```
8309          <port>22</port>
8310      </destination>
8311      <descr><! [CDATA[Test to port 22]]></descr>
8312      <created>
8313          <time>1469130278</time>
8314          <username>admin@192.168.17.103</username>
8315      </created>
8316      <updated>
8317          <time>1472170372</time>
8318          <username>admin@192.168.13.135</username>
8319      </updated>
8320      <disabled/>
8321      </rule>
8322      <rule>
8323          <id/>
8324          <tracker>1465935564</tracker>
8325          <type>pass</type>
8326          <interface>lan</interface>
8327          <ipprotocol>inet</ipprotocol>
8328          <tag/>
8329          <tagged/>
8330          <max/>
8331          <max-src-nodes/>
8332          <max-src-conn/>
8333          <max-src-states/>
8334          <statetimeout/>
8335          <statetype>keep state</statetype>
8336          <os/>
8337          <protocol>icmp</protocol>
8338          <source>
8339              <any/>
8340          </source>
8341          <destination>
8342              <any/>
```

```
8343             </destination>
8344         <descr/>
8345         <updated>
8346             <time>1465935564</time>
8347             <username>admin@192.168.17.100</username>
8348         </updated>
8349         <created>
8350             <time>1465935564</time>
8351             <username>admin@192.168.17.100</username>
8352         </created>
8353     </rule>
8354     <rule>
8355         <type>pass</type>
8356         <ipprotocol>inet</ipprotocol>
8357         <descr><! [CDATA[Default allow LAN to any rule] ]></descr>
8358         <interface>lan</interface>
8359         <tracker>0100000101</tracker>
8360         <source>
8361             <network>lan</network>
8362         </source>
8363         <destination>
8364             <any/>
8365         </destination>
8366     </rule>
8367     <rule>
8368         <type>pass</type>
8369         <ipprotocol>inet6</ipprotocol>
8370         <descr><! [CDATA[Default allow LAN IPv6 to any rule] ]></descr>
8371         <interface>lan</interface>
8372         <tracker>0100000102</tracker>
8373         <source>
8374             <network>lan</network>
8375         </source>
8376         <destination>
```

```
8377          <any/>
8378          </destination>
8379      </rule>
8380      <separator>
8381          <wan/>
8382          <lan/>
8383          <floatingrules/>
8384      </separator>
8385          <bypassstaticroutes>yes</bypassstaticroutes>
8386      </filter>
8387      <shaper>
8388      </shaper>
8389      <ipsec/>
8390      <aliases/>
8391      <proxyarp/>
8392      <cron>
8393          <item>
8394              <minute>1,31</minute>
8395              <hour>0-5</hour>
8396              <mday>*</mday>
8397              <month>*</month>
8398              <wday>*</wday>
8399              <who>root</who>
8400              <command>/usr/bin/nice -n20 adjkerntz -a</command>
8401          </item>
8402          <item>
8403              <minute>1</minute>
8404              <hour>3</hour>
8405              <mday>1</mday>
8406              <month>*</month>
8407              <wday>*</wday>
8408              <who>root</who>
8409              <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
8410          </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>
```

```
8446          <who>root</who>
8447          <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
8448 virusprot</command>
8449      </item>
8450      <item>
8451          <minute>30</minute>
8452          <hour>12</hour>
8453          <mday>*</mday>
8454          <month>*</month>
8455          <wday>*</wday>
8456          <who>root</who>
8457          <command>/usr/bin/nice -n20 /etc/rc.update_urllables</command>
8458      </item>
8459  </cron>
8460  <wol/>
8461  <rrd>
8462      <enable/>
8463      <category>left=system-
8464 processor&right=&resolution=300&timePeriod=-
8465 1d&startDate=&endDate=&startTime=0&endTime=0&graphType=line&in
8466 vert=true</category>
8467  </rrd>
8468  <load_balancer>
8469      <monitor_type>
8470          <name>ICMP</name>
8471          <type>icmp</type>
8472          <descr><! [CDATA[ ICMP ]]></descr>
8473          <options/>
8474      </monitor_type>
8475      <monitor_type>
8476          <name>TCP</name>
8477          <type>tcp</type>
8478          <descr><! [CDATA[ Generic TCP ]]></descr>
8479          <options/>
8480      </monitor_type>
8481      <monitor_type>
```

```
8482             <name>HTTP</name>
8483             <type>http</type>
8484             <descr><! [CDATA[Generic HTTP]]></descr>
8485             <options>
8486                 <path>/</path>
8487                 <host/>
8488                 <code>200</code>
8489             </options>
8490         </monitor_type>
8491         <monitor_type>
8492             <name>HTTPS</name>
8493             <type>https</type>
8494             <descr><! [CDATA[Generic HTTPS]]></descr>
8495             <options>
8496                 <path>/</path>
8497                 <host/>
8498                 <code>200</code>
8499             </options>
8500         </monitor_type>
8501         <monitor_type>
8502             <name>SMTP</name>
8503             <type>send</type>
8504             <descr><! [CDATA[Generic SMTP]]></descr>
8505             <options>
8506                 <send/>
8507                 <expect>220 *</expect>
8508             </options>
8509         </monitor_type>
8510     </load_balancer>
8511     <widgets>
8512     <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
8513 /sequence>
8514
8515     </widgets>
8516     <openvpn/>
```

```

8517      <dnshaper>
8518          </dnshaper>
8519      <unbound>
8520          <enable/>
8521          <dnssec/>
8522          <active_interface/>
8523          <outgoing_interface/>
8524          <custom_options/>
8525          <hideidentity/>
8526          <hideversion/>
8527          <dnssecstripped/>
8528      </unbound>
8529      <dhcpdv6>
8530          <lan>
8531              <range>
8532                  <from>::1000</from>
8533                  <to>::2000</to>
8534          </range>
8535          <ramode>assist</ramode>
8536          <rapriority>medium</rapriority>
8537      </lan>
8538  </dhcpdv6>
8539  <cert>
8540      <refid>5720a0502b277</refid>
8541      <descr><! [CDATA[webConfigurator default (5720a0502b277) ]]></descr>
8542      <type>server</type>
8543  <crt>LS0tLS1CRUdJTibDRVJUSUZJQ0FURS0tLS0tCK1JSUZiVENDQkZXZ0F3SUJBZ01CQURBTkJna3
8544 Foa21HOXcwQkFRc0ZBRENcdERFTE1Ba0dBMVVFQmhNQ1ZWTXgKRGpBTUJnT1ZCQWduQ1ZOMF1YUmxFNUkV3RHdZ
8545 RFZRUUhFd2hNYjJoaGJhbDB1VEU0TURzR0ExVUVDaE12Y0daVApavzV6w1NCM1pXSkRiMjVtYVdkMWntRjBiM0
8546 lnVTJwc1ppMVRhV2R1WldRZ1EyVn1kR2xtYVdOaGRHVxhLREftCkJna3Foa21HOXcwQkNRRVdHV0ZrY1dsdVFI
8547 Qm1VMlZ1YzJvdWJHowPZV3hrYjIxagFXNHhIakFjQmdOVkJBTvQKRlhCbVUyVnVjM1V0T1RjeU1HRXdOVEF5WW
8548 pJM056QWVGdzB4TmpBME1qY3hNVEU1TkRSYUZ3MH1NVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
8549 d0pWVXpFT01Bd0dBMVVFQ0JNR1UzUmhkR1V4RVRBUEJnT1ZCQWNNUckNFehZZMkZzYVhSNU1UZ3d0Z11EV1FRS0
8550 V50XdabE5sYm5ObEl1ZGxza052Ym1acFozVn1ZWfJ2Y21CVFpXeG0KTFZoCfoyNWxaQ0JEWlhKMGFxWnBZMkYw
8551 W1Rfb01DWudDU3FHU01im0RRRUpBU1laWvdSdGFxFNUfjR1pUW1c1egpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
8552 dBMVVFQXhNvmNHW1RaVzV6W1MwMU56SXdZVEExTURKaU1qYzNNSU1CCklqQU5CZ2txaGtpRz13MEJBuuVGQUFP
8553 Q0FROEFNSU1CQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFmUE1aVzNMdG
8554 hDODBH0dhZnJENWdqctrwZkNNMh1zbEFPaV1ZK1hDYjdNa2o0dmtTMgpmbz14emNyaDuRnv1aY1BHeXR1a21s
8555 ZWR4bjFWeF16S11zYXZKdn1Kb11RMctNTkx0dkFjYnRhTUFoZjh1ZkRFC1hrc1NVQ0N5YTFrbEYxNWJGZmcyUG

```

8557 E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkJFRJTkx3QUZnd1E5K1BQZkwKVTQzMFBVb3FFbWEwdzU4Q1RZKzZh  
 8558 ZEFiUEhjWGC5SFA0NFQybFNIQ2M1cUp5UTd1K3IyaFZ0N29EN1oxQmdCUApyeXd1SEZwd3J1LytyWEwieEcrcD  
 8559 dwYXI0aHR0UFRCml1NmFqQVVTNmpvN05kOE1QNWPz1kzR0h2ZjhzUU1ECKFRQUJvNE1CaGpDQ0FZSXduDUV1E  
 8560 V1IwVEJBSxdBREFSQmdsZ2hrZ0JdmhDQVFFRUJBTUNCa0F3TxDZs11JWkkQV1iNFFnRU5CQ11XskU5d1pXNV  
 8561 RVMHdnUjJwdVpYSmhkr1ZrSUZobGNuWmxjaUJEWlhKMGFxWnBZMkYw1RBZApcZ05WSFE0RUznUVU3K11LrmNp  
 8562 OFFVSGhTz0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K11LCKzjaThRVUhoU2dMRHY4RUNzY0  
 8563 Nkd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex  
 8564 VUVCeE1JVEC5allXeHBkSGt4T0RBmkJnT1ZCQW9UTDNCbVuYvnVjM1VnZDJWaQpRMj11Wm1sbmRYSmhkRz15SU  
 8565 ZobGJHWXRVMmxuYm1Wa01FTmxjb1JwWm1sal1YUmxFu2d3SmdZSktrWklodmNOCKfRa0JGAGx0WkcxcGJrQnda  
 8566 bE5sYm5ObExteHZZMkzzWkc5dF1XbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU  
 8567 56ZUNBUUF3SFFZRFZSMGxCQ113RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd01G  
 8568 b0RBtkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXjxFpQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRW1PcmtNaTB5M0  
 8569 9PWGtzWEs1cEM2dTd6Uk13WjEvRjYyRu3OD1UOWx4Y01ZelZOTm5Idlg0bXFPRUcKUWJhRU42NEkxOHFud3Zm  
 8570 S2JrREzvRthMR1hSdzBkMnAyTGvmyTD4YTIVsGNHc0xHTktPbkjxb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG  
 8571 c4bGdrvc3dSt1b01DNDJ1bVjkOURCTm1zdFJ4RV1NMkFLQkFsZG1LYStvRUY1VUwwCm43aXpvN1Z4dHJWMTJv  
 8572 TTdyS11RQ05kY00xZkVsEuwvb3ZkUnVpa0F5Wm1VvnFUL1dDZGo3dDdIVG9ob0RFYzEKS1kOvPpSmR2QmZLVU  
 8573 1sUW1ELyswsvpTa1FXRdczWkdsaeHTk2tOeWc1aDjhUjUwYjh3Wm9zQnNjSUZDa0pFbogp0UT09Ci0tLS0tRUE  
 8574 iENFU1RJRk1DQVRFLS0tLS0K</crt>  
 8575 <prv>LS0tLS1CRUDJTiBQuk1WQVRFIETFWS0tLS0tck1JSUV2Z01CQURBTkJna3Foa21HOXcwQkFRRU  
 8576 ZBQVNDQktd2dnU2tBz0VBQW9JQkFRQzM4NzJIMkE1M01hY1kKMjN3YkNKR1htWFJWky9odVVKeFdsc3hx3M4  
 8577 eGxiY3UyRUX6UVpJWnArc1BtQ09yaWw4SxpUS31VQTZKaGo1YwpKdnN5U1Bpk1JMWithqM0h0eXVIBjdsaxGxzOG  
 8578 JLMjZTS1Y1M0dmV1hGak1saXhxOG0vSW1oaERUNHcwdTI4Qnh1CjFvd0NGL3k10E1SZVN0S1FJTEpyV1NVWFhs  
 8579 c1YrRFk5cmpGMmpZNDdrSE1iU1JZSwxLUHo1TzVtNTA5TW cwdkEKQVdEQkQzNDg50HRAulhROVNpb1NaclREbn  
 8580 dKTmo3cHAwQnM4ZHH1RDBjL2poUGFWsWNKem1vbkpEdDc2dmFGw0zdWdQcG5VR0FFK3ZMQzRjv25DdTcvNWRj  
 8581 dHZFYjZudWxxdm1HMjA5Tut1SzdwC1CUkxxT2pzMTN3Zy9tT31CCmpjWWU5L314QWdNQkFBRUNnZ0VCQUpRRF  
 8582 pxU3duMnNTUTH0SVNBTVUvUW0zcXhrb3BzdzB4cWNScmFl0ED4VmQKejBpOU1KbkZVQWFleTQvL3J1dnzhZW1P  
 8583 R3RYSmZ2ai9jSny3cmJIWGIzYkjtVW9hcDhxY0RjdVSMmlHRUZYWQpCL3hjNvpINTlaTUFabWE1VWVQLzNjcd  
 8584 1zNVhhcHNpc1NXV1I4cFFZc3Z6Mmt6ci8zMXdrQxd4SGJzWHzJVDk1CjNLRmk4VTZUM1hnU1c2eFowZhp1Zn1P  
 8585 UzAvbXlmNU5YLzVoRk1PNmFDc0x1UjZ4N1Rza2FDQu9FY1ViT29qUXkKc09XeWphbEtTUWz3WEzdVM0bXdyR2  
 8586 hMz0NRY1B2MnE5V0Niav0VMNEZUzmRz1ZXchBRNG1ZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZ1F2  
 8587 YTVqYUgyRm5LdkExR2YxY05hGRVQ2dZRUE0NzNMUwoxcExLsmRZN2JxCmtMU3NVT0zhtUZ1ZG1xU2ttbz3Qj  
 8588 1pMXhzBElLQuD0M3U4dTdMz1ZtU21ybnMwVVBTMHRVUDRyQXmzVFJocEgkU2Z4VXVsbgVGGaKtjZk9xRE11TTBC  
 8589 OGttbFJnUFRmVHVPaGNwMGVkmQwK1E5Y2V1Y25kaFp3UE16Tuc3TWRTSApKOG5yU2t5TfdMdWuXuvJNZHnbm  
 8590 NBRDhVYThDz11fQXpzyjYzbzRBSH1YNjZkcEJ6TG1zYzZxS2d2ZG4xazhVcm02N3RuK2M3NkVhSEtzt1k0rjd  
 8591 S0dFSk1ye0yQTJTe1Azdm03Rmk4eGRtblgrsxd5cux5t1VwsnZxQ012TVIKRDFpNWVFTVvoZvo2OUpOK013Sm  
 8592 z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDnsTHvtQOpJZm1DW1pRSUQ1OENnWUJjamFO  
 8593 dk5obnFJOG9rWGHBUjR2c3NtNgpWb0tYU1ZScjRIVHo5MDfwOGdReXNCWkt0Cn1US2V6VThuUVZvTjNYWmVmBc  
 8594 8rVEcwYVpKOTZHky9nNTRWZmZqWTRle1VScHhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3  
 8595 QWY5Mi9CbHzJR25FS1pMdnhLWTdvmx1Ib1NRLzczUG1DSnFqemd6UutCZ1FDZgpJQjE3RzRnWWNGL3hpDGJNTn  
 8596 VudmNUUjZxtzR0ekZtdG5TYWN3W1Ftb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUTU  
 8597 RG1hZGsvKy9Ud2UvVkjBmx2TW9zS3VjTG42Y1c2eGvhR1hFc3FoUj1hbkwzRjMKcEpUSGg4Y3FsNTdqdRkRRN0  
 8598 FBamdyQmxrb3pOVnNMZThiWWpkcHR1MVBRs0JnQ0xDR0R1RXNBYUxwZ1RtOG44bgoYQ1h1NE52K113a1Rlcdu  
 8599 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cvJqeFEvSDgxMHRGd1p3C9uSVDycnRCZ1ZLC1UzSThhYnpnUUt2OEwrZj  
 8600 VadTAxY1pZvk5TU0FIUFRHYm5jb1IzbGPYjNLeUVXQjdsZFBHQwpOS3UwNkd5TEkKah5TDhadEFBRXVBZ1FU  
 8601 OVFOVGJkQWJrCi0tLS0tRUE5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>  
 8602  
 8603 </cert>  
 8604 <revision>  
 8605 <time>1493655499</time>  
 8606 <description><![CDATA[admin@10.97.67.135: /firewall\_rules\_edit.php made  
 8607 unknown change]]></description>  
 8608 <username>admin@10.97.67.135</username>  
 8609 </revision>  
 8610 <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          <unqid>57bf05ffdcc3c</unqid>
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

<b>AD</b>	Active Directory
<b>ARM</b>	Access Rights Management
<b>CA</b>	Certificate Authority
<b>CSF</b>	Cybersecurity Framework
<b>FBA</b>	Forms Based Authentication
<b>GPO</b>	Government Printing Office, Group Policy Object (depending on context)
<b>GUI</b>	Graphical User Interface
<b>HTCC</b>	HyTrust CloudControl
<b>IdAM</b>	Identity and Access Management
<b>IT</b>	Information Technology
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>LDAPS</b>	Lightweight Directory Access Protocol (Secure)
<b>NCCoE</b>	National Cybersecurity Center of Excellence
<b>NIST</b>	National Institute of Standards and Technology
<b>PEP</b>	Policy Enforcement Point
<b>RMF</b>	Risk Management Framework
<b>SA</b>	Situational Awareness
<b>SCM</b>	Security Compliance Manager
<b>SIEM</b>	Security Information and Event Management
<b>RDP</b>	Remote Desktop Protocol
<b>VD</b>	Virtual Directory
<b>VDS</b>	Virtual Directory System
<b>VM</b>	Virtual Machine
<b>VNC</b>	Virtual Network Computing
<b>VPN</b>	Virtual Private Network