

NIST SPECIAL PUBLICATION 1800-9

Access Rights Management for the Financial Services Sector

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), and How-To Guides (C)

James Banoczi
Sallie Edwards
Nedu Irrechukwu
Josh Klosterman
Harry Perper
Susan Prince
Susan Symington
Devin Wynne

DRAFT

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



NIST SPECIAL PUBLICATION 1800-9

Access Rights Management for the Financial Services Sector

*Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B),
and How-To Guides (C)*

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*

DRAFT

August 2017



U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Kent Rochford, Acting Undersecretary of Commerce for Standards and Technology and Director

Access Rights Management for the Financial Services Sector

Volume A:
Executive Summary

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>

1 Executive Summary

- 2 ▪ The NCCoE has developed an example implementation that demonstrates ways in which a financial
3 services company can improve their information system security by limiting employee access to
4 only the information they need to do their job, at the time they need it, and nothing more.
5 Essentially, enabling a company to give the right person the right access to the right resources at
6 the right time.
- 7 ▪ Specifically, this project provides an example solution that describes how to execute changes and
8 coordinate employee access to data and systems quickly, simultaneously, and consistently—and in
9 accordance with corporate access policies.
- 10 ▪ Today’s threat landscape has created ever-increasing challenges for financial services companies as
11 they work to protect important financial assets and customer data. Financial services companies
12 are under a high and sustained level of attack, in some instances experiencing a direct loss. Costs
13 associated with these cyber attacks are growing and have reached an average loss of one million
14 dollars per incident.*
- 15 ▪ Complicating efforts to protect important data is the highly complex infrastructure that established
16 financial services companies must manage. Disparate, legacy systems that run on different
17 operating platforms are difficult to manage and ensure appropriate levels of access management.
- 18 ▪ To combat these challenges, various regulatory organizations, such as the FFIEC as well as other
19 federal, state, and other industry organizations, have developed a range of compliance mandates
20 for financial services companies. As an example, financial services companies should apply the
21 principles of least privilege to grant employee access to systems and data. This guide acknowledges
22 these compliance requirements.
- 23 ▪ A properly implemented and administered Access Rights Management (ARM) system can help your
24 organization meet compliance requirements, limit opportunity for and reduce the damage of an
25 attack, and improve enforcement of enterprise information system access policies.

26 CHALLENGE

27 Managing user access in a fast-moving industry such as the financial services sector requires frequent
28 changes to user identity and role information and to user access profiles for systems and data. Employees
29 using these various ARM systems may lack methods to coordinate access across the corporation effectively
30 to ensure that ARM changes are executed consistently throughout the enterprise. This inconsistency is
31 inefficient and can result in security risks. See Section 1.3 for the risk factors addressed by the solution.

32 Many financial services companies use ARM systems that are fragmented and controlled by numerous
33 departments. For example, changes to user identity and role information should be managed by an ARM
34 system within the Human Resources department; changes to user access profiles may be managed by IT
35 system administrators; and changes to user access profiles for specific resources or data may be managed
36 by still other systems under the control of various business unit managers.

37 In collaboration with experts from the financial services sector and technology collaborators that provided
38 the requisite equipment and services, we developed representative use-case scenarios to describe user

* *Kaspersky Lab Report 2017, New Technologies, New Cyberthreats: Analyzing the state of IT Security in financial sector*
https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf

39 access security challenges based on normal day-to-day business operations. The use cases include user
40 access changes (e.g., promotion or transfer between departments), new user onboarding, and employees
41 leaving an institution.

42 **SOLUTION**

43 The NCCoE developed an ARM system that executes and coordinates changes across the enterprise ARM
44 systems to change the employee’s access for all data and systems quickly, simultaneously, and consistently,
45 according to corporate access policies. The example implementation provides timely management of access
46 changes and reduces the potential for errors. It also enhances the security of the directories. Generally, an
47 ARM system enables an institution to give the right person the right access to the right resources at the
48 right time. The ARM reference design and example implementation are described in this NIST Cybersecurity
49 “Access Rights Management” practice guide.

50 Financial services companies can use some or all of the guide to implement an ARM system. The guide
51 references NIST guidance and industry standards, including the Federal Financial Institutions Examination
52 Council Cybersecurity Assessment Tool (FFIEC CAT). The NCCoE used commercial, standards-based products
53 that are readily available and interoperable with commonly used IT infrastructure and investments. We
54 built an environment that simulates a financial services company’s infrastructure. The infrastructure
55 includes the typical network segmentation and IT components (i.e., virtual infrastructure, directories, etc.).
56 Simulated financial systems (banking and loan operations systems) further illustrate the solution.

57 The NCCoE reference design includes the following capabilities:

- 58 ▪ A single system that is capable of interacting with multiple existing access management systems for
59 a complete picture of access rights within the organization
- 60 ▪ Secure communications between all components
- 61 ▪ Automated logging, reporting, and alerting of identity and access management events across the
62 enterprise
- 63 ▪ Ad hoc reporting to answer management, performance, and security questions
- 64 ▪ Support for multiple access levels for the ARM system (e.g., administrator, operator, viewer)
- 65 ▪ Protection from the introduction of new attack vectors into existing systems
- 66 ▪ A complement to, rather than replacement of, existing security infrastructure

67 While we have used a suite of commercial products to address this challenge, this guide does not endorse
68 these particular products, nor does it guarantee compliance with any regulatory initiatives. Your
69 organization's information security experts should identify the products that will best integrate with your
70 existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to
71 these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts
72 of a solution.

73 **BENEFITS**

74 The NCCoE’s practice guide to address Access Rights Management for the financial services sector can help
75 your organization:

- 76 ▪ Reduce damage caused by a successful insider threat attack by limiting the amount of data to which
77 any one person has access
- 78 ▪ Limit opportunity for a successful attack by reducing the available attack surface
- 79 ▪ Increase the probability that investigations of attacks or anomalous system behavior will reach
80 successful conclusions
- 81 ▪ Reduce complexity, which leads to:
 - 82 • Faster and more accurate access policy modifications
 - 83 • Fewer policy violations due to access inconsistencies
- 84 ▪ Simplify compliance by producing automated reports and documentation

85 **SHARE YOUR FEEDBACK**

86 View or download the guide at https://nccoe.nist.gov/projects/use_cases/access_rights_management.
87 Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt
88 this solution for your own organization, please share your experience and advice with us. We recognize that
89 technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to
90 share lessons learned and best practices for transforming the processes associated with implementing
91 these guidelines.

92 To provide comments or to learn more by arranging a demonstration of this reference solution, contact the
93 NCCoE at financial_nccoe@nist.gov.

94 **TECHNOLOGY PARTNERS/COLLABORATORS**

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



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

104 The National Cybersecurity Center of Excellence (NCCoE), a part of the National
105 Institute of Standards and Technology (NIST), is a collaborative hub where
industry organizations, government agencies, and academic institutions work
together to address businesses' most pressing cybersecurity challenges.
Through this collaboration, the NCCoE applies standards and best practices to
develop modular, easily adaptable example cybersecurity solutions using
commercially available technology.

LEARN MORE

Visit <https://nccoe.nist.gov>
nccoe@nist.gov
301-975-0200

Access Rights Management for the Financial Services Sector

Volume B:
Approach, Architecture, and Security Characteristics

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>

DRAFT

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 1800-9B Natl. Inst. Stand. Technol. Spec. Publ. 1800-9B, 104 pages, August 2017 CODEN: NSPUE2

FEEDBACK

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

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

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

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

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

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

64 **Contents**

65 **1 Summary..... 1**

66 1.1 Challenge 1

67 1.2 Solution..... 2

68 1.3 Risk Considerations 3

69 1.4 Benefits..... 3

70 **2 How to Use This Guide..... 4**

71 2.1 Typographical Conventions 5

72 **3 Approach..... 6**

73 3.1 Audience..... 6

74 3.2 Scope 6

75 3.3 Assumptions..... 7

76 3.3.1 Security 7

77 3.3.2 Modularity..... 7

78 3.3.3 Human Resources Database/Identity Vetting..... 7

79 3.3.4 Technical Implementation 7

80 3.3.5 Limited Scalability Testing..... 8

81 3.3.6 Replication of Enterprise Networks..... 8

82 3.4 Risk Assessment..... 8

83 3.4.1 Assessing Risk Posture 8

84 3.4.2 Security Control Map 9

85 3.5 Security Functions and Subcategories Related to FFIEC..... 26

86 3.6 Technologies..... 29

87 **4 Architecture..... 34**

88 4.1 Architecture Description 34

89 4.1.1 High-Level Architecture 34

90 4.1.2 Reference Design..... 35

91 **5 Example Implementation..... 39**

92	5.1	Example Implementation Description.....	39
93	5.2	Operation of the Example Implementation	41
94	5.2.1	Example Implementation Network Components Overview	43
95	5.2.2	Common Services Network.....	45
96	5.2.3	Access Rights Management Network.....	45
97	5.2.4	Network Data Flows	46
98	5.3	Data	49
99	6	Security Analysis.....	50
100	6.1	Assumptions and Limitations.....	50
101	6.2	Build Testing.....	50
102	6.3	Scenarios and Findings	50
103	6.4	Analysis of the Reference Design’s Support for CSF Subcategories	51
104	6.4.1	Supported CSF Subcategories	56
105	6.5	Security of the Reference Design.....	64
106	6.5.1	Securing New Attack Surfaces.....	68
107	6.5.2	Ensuring Information Integrity.....	70
108	6.5.3	Privileged Access Management.....	70
109	6.5.4	Isolating Reference Design Capabilities from Each Other	71
110	6.5.5	Deployment Recommendations.....	73
111	6.6	Security Evaluation Summary.....	76
112	7	Functional Evaluation.....	78
113	7.1	ARM Functional Test Plan.....	78
114	7.2	ARM Use Case Requirements	79
115	7.3	Test Case: ARM-1	84
116	7.4	Test Case ARM-2	86
117	7.5	Test Case ARM-3	88
118	7.6	Test Case ARM-4	90
119	7.7	Test Case ARM-5.....	92
120		Appendix A List of Acronyms.....	94

121	Appendix B Legend for Diagrams.....	95
122	Appendix C References	96

123 **List of Figures**

124 **Figure 4-1 ARM High-Level Architecture 34**

125 **Figure 4-2 ARM Reference Design 36**

126 **Figure 5-1 Example Implementation 40**

127 **Figure 5-2 Example Implementation Data Flow 42**

128 **Figure 5-3 Monitoring Data Flow 43**

129 **Figure 5-4 ARM Example Implementation Network 44**

130 **Figure 5-5 Common Services Network 45**

131 **Figure 5-6 ID-ARM Network..... 46**

132 **Figure 5-7 User Access Information Network Data Flow (Steps 1 and 2 in Figure 5-2) 47**

133 **Figure 5-8 User Access Information Network Data Flow (Step 3 in Figure 5-2) 48**

134 **Figure 5-9 Monitoring Network Data Flow..... 49**

135 **List of Tables**

136 **Table 3-1 ARM Reference Design CSF Core Components Map 11**

137 **Table 3-2 FFIEC CAT Guidance 26**

138 **Table 3-3 Products and Technologies..... 29**

139 **Table 5-1 Example Implementation Component List 39**

140 **Table 6-1 ARM Reference Design Capabilities and Supported CSF Subcategories..... 52**

141 **Table 6-2 Capabilities for Managing and Securing the ARM Reference Design 65**

142 **Table 7-1 Test Case Fields 79**

143 **Table 7-2 ARM Functional Requirements..... 80**

144 **Table 7-3 Test Case ID: ARM-1 84**

145 **Table 7-4 Test Case ID: ARM-2 86**

146 **Table 7-5 Test Case ID: ARM-3 88**

147 **Table 7-6 Test Case ID: ARM-4 90**

148 **Table 7-7 Test Case ID: ARM-5 92**

149 **1 Summary**

150 The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and
151 Technology (NIST) addresses the challenge to provide a more secure and efficient way to manage access
152 to data and systems. The NCCoE developed a reference design and an example implementation for this
153 problem using commercially available products. This approach delivers an Access Rights Management
154 (ARM) system that coordinates changes throughout the enterprise, thereby reducing the risk of
155 unauthorized access caused by malicious actors or human error. Throughout this practice guide, access
156 is used as a generic term for privileges and permissions to view, modify, and delete data, applications,
157 and systems.

158 This example implementation is documented as a NIST Cybersecurity Practice Guide, a how-to handbook
159 that presents instructions to implement an ARM system using standards-based, cybersecurity
160 technologies in the real world. Based on risk analysis and regulatory guidance, this design is intended to
161 help companies gain efficiencies in ARM, while saving money and time during the research and proof-of-
162 concept phases of a project. This guide presents an architecture for implementing an ARM that
163 improves the control of user access information using automation. It also quickly identifies unapproved
164 changes such as privilege escalations by including multiple methods of monitoring the user access
165 information repositories (directories).

166 **1.1 Challenge**

167 Managing user access in a fast-moving industry such as the financial services sector requires frequent
168 changes to user identity and role information and to user access profiles for systems and data.
169 Employees using these various ARM systems may lack methods to coordinate access across the
170 corporation effectively to ensure that ARM changes are executed consistently throughout the
171 enterprise. This inconsistency is inefficient and can result in security risks. See [Section 1.3](#) for the risk
172 factors addressed by the solution.

173 Many financial services companies use ARM systems that are fragmented and controlled by numerous
174 departments. For example, changes to user identity and role information should be managed by an ARM
175 system within the human resources (HR) department; changes to user access profiles may be managed
176 by IT system administrators; and changes to user access profiles for specific resources or data may be
177 managed by still other systems under the control of various business unit managers.

178 In collaboration with experts from the financial services sector and collaboration partners that provided
179 the requisite equipment and services, we developed representative use-case scenarios to describe user
180 access security challenges based on normal day-to-day business operations. The use cases include user
181 access changes (e.g., promotion or transfer between departments), new user onboarding, and
182 employees leaving a company.

183 1.2 Solution

184 The NCCoE developed an ARM system that executes and coordinates changes across the enterprise ARM
185 systems to change the employee’s access for all data and systems quickly, simultaneously, and
186 consistently, according to corporate access policies. The example implementation provides timely
187 management of access changes and reduces the potential for errors. It also enhances the security of the
188 directories. Generally, an ARM system enables a company to give the right person the right access to the
189 right resources at the right time. The ARM reference design and example implementation are described
190 in this NIST Cybersecurity “Access Rights Management” Practice Guide.

191 Financial sector companies can use some or all of the guide to implement an ARM system. The guide
192 references NIST guidance and industry standards, including the Federal Financial Institutions
193 Examination Council Cybersecurity Assessment Tool (FFIEC CAT). The NCCoE used commercial,
194 standards-based products that are readily available and interoperable with commonly used IT
195 infrastructure. We built an environment that simulates a financial services company’s infrastructure. The
196 infrastructure includes the typical network segmentation and IT components (i.e., virtual infrastructure,
197 directories, etc.). Simulated financial systems (banking and loan operations systems) further illustrate
198 the solution.

199 In the sections that follow, we show how a financial services company can implement an ARM platform
200 using commercially available products to provide a comprehensive management platform for all user
201 access information within the company. As part of the planning process to deploy an ARM system, an
202 organization will have the opportunity to audit the access control information in their directories and
203 get a more global, correlated, disambiguated view of the user access roles and attributes that are
204 currently in effect. User access information includes directory accounts, group membership, and
205 attributes independent of the use of Active Directory or other directory products. We chose the term
206 *user access information* because it is transparent to non-technical readers.

207 This practice guide:

- 208 ▪ Maps security capabilities of the reference design to guidance and best practices from NIST,
209 International Organization for Standardization (ISO) and by the International Electrotechnical
210 Commission (IEC), and the FFIEC CAT
- 211 ▪ Delivers:
 - 212 • a detailed reference design
 - 213 • an example implementation that is modular and can be implemented using different
214 products to achieve the same results
 - 215 • instructions for implementers and security engineers, including examples of all the
216 necessary components and installation, configuration, and integration information

- 217 • an example implementation that uses products that are readily available and interoperable
218 with existing information technology infrastructure
- 219 • solutions that can meet the needs of financial services companies of all sizes

220 Although the example implementation is built from a suite of commercial products, this practice guide
221 does not endorse these particular products. A company’s IT personnel should identify the standards-
222 based products that will best integrate with its existing tools and infrastructure. Companies can adopt
223 this solution or one that adheres to these guidelines in whole, or they can use this guide as a starting
224 point for tailoring and implementing parts of the solution.

225 The reference design and example implementation support efforts to comply with financial services
226 sector regulations. However, implementation of the reference design or example implementation does
227 not imply or guarantee regulatory compliance.

228 **1.3 Risk Considerations**

229 Members of the financial services sector identified risk factors at both the operational and strategic
230 levels. Operationally, the absence of an ARM platform can increase the risk of compromise of the
231 confidentiality, integrity, and availability of the corporate systems and data.

232 At the strategic level, an organization might consider the cost of mitigating these risks and the potential
233 return on investment from implementing a product (or multiple products). It may also want to assess if
234 an ARM system can help enhance the productivity of employees, speed delivery of services, or explore
235 the potential to support oversight of resources, including IT, personnel, and data. We review the
236 potential benefits of the reference design in Section 1.4.

237 We understand that introducing new technology into any environment may introduce new attack
238 vectors. In addition, converging ARM functions concentrates control over the modifications to user
239 access information. We address these key risk areas and provide a comprehensive list of mitigations in
240 [Section 6, Security Analysis](#).

241 **1.4 Benefits**

242 The reference design and example implementation has the following benefits:

- 243 ▪ reduces the risk of malicious or untrained people gaining unauthorized access to systems and
244 data
- 245 ▪ allows rapid automated provisioning and de-provisioning of user access information, freeing up
246 system administrators to address more critical tasks
- 247 ▪ improves management of user access information changes
- 248 ▪ rapidly identifies anomalous user account changes

- 249 ▪ can be integrated into an organization’s existing infrastructure in whole or in part

250 **2 How to Use This Guide**

251 This NIST Cybersecurity Practice Guide demonstrates a standards-based reference design and provides
252 users with the information they need to replicate this approach to ARM. This reference design is
253 modular and can be deployed in whole or in parts.

254 This guide contains three volumes:

- 255 ▪ NIST SP 1800-9A: *Executive Summary*
256 ▪ NIST SP 1800-9B: *Approach, Architecture, and Security Characteristics*—what we built and why
257 **(you are here)**
258 ▪ NIST SP 1800-9C: *How-To Guide*—instructions for building the example solution

259 Depending on their role in an organization, readers might use this guide in different ways:

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

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

265 **Technology or security program managers** who are concerned with how to identify, understand, assess,
266 and mitigate risk will be interested in this part of the guide, *NIST SP 1800-9B*, which describes what we
267 did and why. The following sections will be of particular interest:

- 268 ▪ [Section 3.4, Risk Assessment](#), provides a description of the risk analysis we performed.
269 ▪ [Section 3.4.2, Security Control Map](#), maps the security characteristics of this example solution to
270 cybersecurity standards and best practices.

271 The *Executive Summary, NIST SP 1800-9A*, could be shared with the leadership team members to help
272 them understand the importance of adopting standards-based ways to manage access to data and
273 systems in a secure and efficient manner.

274 **IT professionals** who want to implement an approach like this will find the whole practice guide useful.
275 The How-To portion of the guide, *NIST SP 1800-9C*, can be used to replicate all or parts of the build
276 created in our lab. The How-To guide provides specific product installation, configuration, and
277 integration instructions for implementing the example solution. We do not re-create the product
278 manufacturers’ documentation, which is generally widely available. Rather, we show how we
279 incorporated the products in our environment to create an example solution.

280 This guide assumes that IT professionals have experience implementing security products within the
281 enterprise. While we have used a suite of commercial products to address this challenge, this guide does

282 not endorse these particular products. An organization can adopt this solution or one that adheres to
 283 these guidelines in whole, or it can use this guide as a starting point for tailoring and implementing parts
 284 of an ARM solution. An organization’s security experts should identify the products that will best
 285 integrate with its existing tools and IT system infrastructure. We hope organizations will seek products
 286 that are congruent with applicable standards and best practices. [Section 3.6, Technologies](#), lists the
 287 products we used and maps them to the cybersecurity controls provided by this reference solution.

288 A *NIST Cybersecurity Practice Guide* does not describe “the” solution, but a possible solution. This is a
 289 draft guide. We seek feedback on its contents and welcome input. Comments, suggestions, and success
 290 stories will improve subsequent versions of this guide. Please contribute comments using email
 291 financial_nccoe@nist.gov or online via the web content tool.

292 2.1 Typographical Conventions

293 The following table presents the typographic conventions used in this volume.

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

294 **3 Approach**

295 This project began with a detailed discussion between NCCoE and members of the financial services
296 sector community about their security challenges around implementing least privilege and separation of
297 duty policies. The principle of least privilege, defined as providing the least amount of access (to systems
298 or data) necessary for the user to complete his or her job [1], and the principle of separation of duties,
299 which restricts the amount of responsibilities held by any one individual, are important security tools.
300 The focus of the project became the risk impacts that result from user access information updates not
301 being implemented consistent with corporate access policies. The NCCoE drafted a use case (i.e., project
302 description) that identified the solution security controls with feedback from the financial industry. After
303 an open call in the Federal Register, technology partners volunteered products, services, and resources
304 that provide the desired security controls. The following sections describe the areas of discussion that
305 led to the development of the subject of this practice guide, including the areas of the NIST
306 Cybersecurity Framework (CSF) and FFIEC CAT.

307 **3.1 Audience**

308 This practice guide is intended for individuals or entities interested in understanding the ARM reference
309 design and example solution the NCCoE designed and implemented. The guide describes how financial
310 services companies (or any other sector organization) can add automation to existing identity and access
311 management (IdAM) systems. In addition, the guide describes how to add IdAM monitoring for
312 anomalous identity and access management system changes, such as unauthorized privilege escalations.

313 **3.2 Scope**

314 We determined that the scope should be ARM, including a converged provisioning component. The
315 scope was further refined to include successful execution of the following provisioning functions:

- 316 ▪ enabling access for a new employee
- 317 ▪ modifying access for an existing employee (including converting an ex-employee to contractor
318 status)
- 319 ▪ disabling access for a terminated employee
- 320 ▪ identifying anomalous directory changes

321 The objective of the project is to perform any of these three access change actions from a single
322 management system that can provision user access information changes to all directories (authoritative
323 sources) within a financial services company. The actions can be initiated via an administrative interface
324 by an approved administrator or via a bulk update from a human resource system. In addition, a
325 Monitoring capability was implemented to enhance the security of the directories.

326 Although the example implementation can provide an approval workflow to ensure that proper
327 management governance is followed, this optional feature was not implemented. Note also that the
328 project does not address access policy decision and enforcement, and identity validation and credential
329 management.

330 3.3 Assumptions

331 3.3.1 Security

332 All network and system changes have the potential to increase the attack surface within an enterprise.
333 Therefore, it is important that the reference design itself be secured to minimize any risks that may
334 otherwise be inherent in its adoption. In the ARM security analysis ([Section 6](#)), we identify the security
335 functions and controls that the reference design supports ([Section 6.4](#)), and we also discuss the security
336 of the reference design itself ([Section 6.5](#)). We assume that all potential adopters of the reference
337 design will implement network security policies. The assessment focuses on how risk factors introduced
338 by the reference design itself are mitigated. We also recommend ways to secure the reference design
339 deployment. However, our evaluation cannot identify all weaknesses, especially those that a specific
340 deployment or specific commercial products may introduce.

341 3.3.2 Modularity

342 As noted, this example implementation uses commercially available products. Organizations can swap
343 any of the products we used for ones better suited for their environment. A combination of some or all
344 the components described here, or a single component, can improve the security of identity and access
345 management functions without requiring an organization to remove or replace its existing
346 infrastructure. In addition, organizations may find that we describe new ways to use currently deployed
347 components.

348 3.3.3 Human Resources Database/Identity Vetting

349 We assume that a company has a user change process, databases, and other components necessary to
350 establish a valid identity.

351 3.3.4 Technical Implementation

352 This practice guide is written from a how-to perspective and aims to provide details on how to design,
353 install, configure, and integrate components. We assume that financial services companies have the
354 technical resources to implement all or parts of the example implementation or have access to
355 companies that can perform the implementation on its behalf. The guide may also provide insights
356 regarding the level of effort and types of resources required to accomplish an ARM implementation.

357 3.3.5 Limited Scalability Testing

358 We did not attempt to replicate the user base size that would be found in most companies. We do not
359 identify scalability thresholds in our ARM example implementation because they depend on the type
360 and size of the implementation and are particular to the individual enterprise. We believe the reference
361 design can be applied to any size company because it can be implemented in a modular fashion and is
362 based on standards.

363 3.3.6 Replication of Enterprise Networks

364 We were able to replicate the typical information technology or corporate network in a limited manner.
365 The goal was to demonstrate that provisioning functions could be performed from an ARM system
366 regardless of its location in the enterprise. In a real-world environment, the interconnections between
367 enterprise subnetworks depend on the business needs and compliance requirements of the enterprise.
368 We did not attempt to replicate these interconnections. Rather, we acknowledge that implementing our
369 example implementation or its components creates new interfaces across subnetworks.

370 3.4 Risk Assessment

371 [NIST SP 800-30 Rev. 1, Risk Management Guide for Information Technology Systems](#), defines risk as "a
372 measure of the extent to which an entity is threatened by a potential circumstance or event, and
373 typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and
374 (ii) the likelihood of occurrence." The NCCoE recommends that any discussion of risk management,
375 particularly at the enterprise level, begin with a comprehensive review of [NIST 800-37, Guide for](#)
376 [Applying the Risk Management Framework to Federal Information Systems](#). The risk management
377 framework (RMF) guidance, as a whole, proved invaluable in giving us a baseline to assess risks, from
378 which we developed the project, the required security controls of the reference design, and this guide.

379 We performed two types of risk assessment:

- 380 ▪ initial analysis of the risk factors discussed with the financial services companies, which led to
381 the creation of the use case and the desired security posture
- 382 ▪ analysis of how to secure the capabilities within the solution and minimize any vulnerabilities
383 that they might introduce (see [Section 6, ARM Security Analysis](#))

384 3.4.1 Assessing Risk Posture

385 Using the guidance in NIST's series of publications concerning risk, we worked with financial services
386 companies and the Financial Sector Information Sharing and Analysis Center (FS-ISAC) to identify the
387 most compelling risk factors that financial services companies encounter. We participated in
388 conferences and met with members of the financial services sector to define the main security risks to
389 business operations. These discussions resulted in the identification of a primary risk area—the lack of

390 automated ARM capabilities. We then identified the following threats that an ARM system can help
391 mitigate:

- 392 ▪ insiders gaining access through access creep and undocumented accounts
- 393 ▪ regular users unintentionally accessing unauthorized data or systems
- 394 ▪ external actors gaining access by using malware techniques

395 These discussions also gave us an understanding of the vulnerabilities that threat actors can exploit due
396 the lack of automated ARM capabilities. We identified the following vulnerabilities:

- 397 ▪ undocumented accounts
- 398 ▪ accounts with unnecessarily elevated privileges
- 399 ▪ dependence on humans to enforce user access policies

400 These risk factors can also be viewed from a business operations risk perspective:

- 401 ▪ impact on service delivery—ensuring that people have access only to the systems they need to
402 perform their job functions reduces the risk of inappropriate or unauthorized use of access that
403 could then affect availability to others
- 404 ▪ cost of implementation—implementing ARM once and using it across all systems may reduce
405 both system development costs and operational costs
- 406 ▪ compliance with existing industry standards—FFIEC requires deliberate and timely control of
407 logical access to corporate resources
- 408 ▪ maintenance of reputation and public image

409 We subsequently translated the risk factors identified to security functions and subcategories within the
410 NIST CSF and the FFIEC CAT that the design needed to support. We also mapped the categories to NIST’s
411 SP 800-53 Rev.4 [2] controls and IEC/ISO controls for additional guidance in Table 3-1.

412 3.4.2 Security Control Map

413 As explained in Section 3.4.1, we identified the CSF security functions and subcategories that we wanted
414 the reference design to support through a risk analysis process conducted in collaboration with our
415 financial services sector stakeholders. This was a critical first step in designing the reference design and
416 example implementation to mitigate the risk factors. Table 3-1 lists the addressed CSF functions and
417 subcategories and maps them to relevant NIST standards, industry standards, controls, and best
418 practices, including those published by FFIEC. The items in the FFIEC Examination Handbook column of
419 Table 3-1 are mapped from and reflect the FFIEC Cybersecurity Assessment Tool, dated June 2015,
420 Appendix A – Mapping Baseline Statements to FFIEC IT Examination Handbook. The references provide
421 solution validation points in that they list specific security capabilities that a solution addressing the CSF
422 subcategories would be expected to exhibit.

423 Organizations can use Table 3-1 to identify the CSF subcategories and NIST 800-53 controls or FFIEC
424 guidance that they are interested in addressing. Note that not all the CSF subcategories or FFIEC
425 guidance can be implemented using technology. The subcategories that describe processes and
426 organizational policies are supported by the reference design, not implemented. Therefore, any
427 organization adopting an ARM solution would need to develop and implement specific processes that
428 address those processes and policies. For example, some of the subcategories within the CSF function
429 “Identify” are processes and policies that should be developed prior to an ARM implementation.

430 Table 3-1 ARM Reference Design CSF Core Components Map

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
ID.AM-3: Organizational communication and data flows are mapped.	AC-4, CA-3, CA-9, PL-8	A.13.2.1	D4.C.Co.Int.1: A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.	IS.B.1.3: Identify changes to the technology infrastructure or new products and services that might increase the institution's risk from information security issues. Consider ... network topology, including changes to configuration or components. IS.B.9: A risk assessment should include an identification of information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information and information systems can be both paper-based and electronic.
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established.	CP-2, PS-7, PM-11	A.6.1.1	D1.R.St.B.1: Information security roles and responsibilities have been identified.	IS.B.7: Employees should know, understand, and be held accountable for fulfilling their security responsibilities. Financial institutions should define these responsibilities in their security policy.

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
<p>ID.BE-4: Dependencies and critical functions for delivery of critical services are established.</p>	<p>SA-14, CP-8, PE-9, PE-11, PM-8, SA-14</p>	<p>A.11.2.2, A.11.2.3, A.12.1.3</p>	<p>D1.G.IT.B.2: Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.</p>	<p>IS.WP.I.4.1: Review and evaluate security policies and standards to ensure that they sufficiently address the risks identified by the institution: software development and acquisition, including processes that evaluate the security features and software trustworthiness of code being developed or acquired, as well as change control and configuration management.</p>

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
<p>PR.AC-1: Identities and credentials are managed for authorized devices and users.</p>	<p>AC-2, IA Family</p>	<p>A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3</p>	<p>D3.PC.Im.B.7: Access to make changes to systems configurations (including virtual machines and hypervisor) is controlled and monitored.</p> <p>D3.PC.AM.B.6: Identification and authentication are required and managed for access to systems, applications, and hardware.</p> <p>D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.</p>	<p>IS.B.56: Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. The steps include maintaining appropriately robust configuration management and change control processes.</p>

<p>PR.AC-3: Remote access is managed.</p>	<p>AC-17, AC-19, AC-20</p>	<p>A.6.2.2, A.13.1.1, A.13.2.1</p>	<p>D3.PC.Am.B.15: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.</p> <p>D3.PC.Im.Int.2: Security controls are used for remote access to all administrative consoles, including restricted virtual systems.</p>	<p>IS.B.45: Financial institutions should secure remote access to and from their systems ... securing remote access devices and using strong authentication and encryption to secure communications.</p> <p>IS.WP.II.B.17: Determine whether remote access devices and network access points for remote equipment are appropriately controlled. For example, authentication is of appropriate strength (e.g., two-factor for sensitive components), and remote access devices are appropriately secured and controlled by the institution.</p> <p>IS.B.56: Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. The steps include maintaining appropriately robust configuration management and change control processes.</p> <p>IS.WP.II.H: Determine whether management explicitly follows a recognized security standard development process or adheres to widely recognized industry standards.</p>
--	----------------------------	--	---	--

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
<p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.</p>	<p>AC-2, AC-3, AC-5, AC-6, AC-16</p>	<p>A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4</p>	<p>D3.PC.Am.B.1: Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. D3.PC.Am.B.2: Employee access to systems and confidential data provides for separation of duties. D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.</p>	<p>IS.B.19: Access rights should be based on the needs of the applicable user to carry out legitimate and approved activities on the financial institution's information systems. IS.WP.I.4.1: Review security policies and standards to ensure that they sufficiently address administration of access rights at enrollment, when duties change, and at employee separation. IS.B.18: Financial institutions should have an effective process to administer access rights, including assigning users and devices only the access required to perform their required functions and updating access rights based on personnel or system changes.</p>

<p>PR.DS-1: Data-at-rest is protected.</p>	<p>SC-28</p>	<p>A.8.2.3</p>	<p>D1.G.IT.B.13: Confidential data is identified on the institution's network.</p> <p>D3.PC.Am.A.1: Encryption of select data-at-rest is determined by the institution's data classification and risk assessment.</p>	<p>IS.B.9: A risk assessment should include an identification of information and the information systems to be protected, including electronic systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information and information systems can be both paper-based and electronic.</p> <p>IS.WP.I.3.1: Consider whether the institution has identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to customer non-public information as well as the risks to the institution.</p> <p>IS.B.12: Prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.</p> <p>IS.B.51: Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information.</p>
---	--------------	----------------	---	---

<p>PR.DS-2: Data-in-transit is protected.</p>	<p>AC-4, SC-8, SC-12, SC-13, SC-17, SC-23, SC-8</p>	<p>A.8.2, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3</p>	<p>D3.PC.Am.B.13: Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).</p> <p>D3.PC.Am.E.5: Controls are in place to prevent unauthorized access to cryptographic keys.</p> <p>D3.PC.Am.Int.7: Confidential data is encrypted in transit across private connections (e.g., frame relay and T1) and within the institution’s trusted zones.</p> <p>D3.PC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used.</p> <p>D3.PC.Im.Int.1: The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.</p>	<p>IS.B.51: Encryption is used to secure communications and data storage, particularly authentication credentials and the transmission of sensitive information.</p> <p>IS.WP.II.B.15: Determine whether appropriate controls exist over the confidentiality and integrity of data transmitted over the network (e.g., encryption, parity checks, message authentication).</p> <p>IS.B.21: Encrypting the transmission and storage of authenticators (e.g., passwords, personal identification numbers (PINs), digital certificates, and biometric templates).</p> <p>IS.B.33: Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as domain name service (DNS). Institutions internally hosting Internet-accessible services should consider implementing additional firewall components that include application-level screening.</p>
--	---	--	---	--

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
				IS.WP.I.4.1: Evaluate the appropriateness of technical controls mediating access between security domains.
PR.DS-5: Protections against data leaks are implemented.	AC-4, AC-5, AC-6, SC-8, SC-13, SI-4	A.6.1.2, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.13.1.3, A.13.2.1, A.13.2.3	D3.PC.Am.Int.1: The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.	IS.B.19: Access rights should be based on the needs of the applicable user to carry out legitimate and approved activities on the financial institution's information systems. IS.WP.I.4.1: Review security policies and standards to ensure that they sufficiently address administration of access rights at enrollment, when duties change, and at employee separation.

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
<p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.</p>	<p>AU Family IR-5, IR-6</p>	<p>A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1</p>	<p>D2.MA.Ma.B.1: Audit log records and other security event logs are reviewed and retained in a secure manner.</p>	<p>IS.B.79: Institutions should strictly control and monitor access to log files whether on the host or in a centralized logging facility.</p> <p>IS.WP.II.B.13: Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period and that reporting to those logs is adequately protected.</p> <p>IS.B.83: Because the identification of incidents requires monitoring and management, response centers frequently use (security information management (SIM) tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents.</p>

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
<p>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. (p. 29).</p>	<p>AC-3, CM-7</p>	<p>A.9.1.2</p>	<p>D3.PC.Am.B.4: User access reviews are performed periodically for all systems and applications based on the risk to the application or system.</p> <p>D3.PC.Am.B.3: Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).</p> <p>D4.RM.Om.Int.1: Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.</p>	<p>IS.B.18: Reviewing periodically users' access rights at an appropriate frequency based on the risk to the application or system.</p> <p>IS.WP.I.7.6: Evaluate the process used to monitor and enforce policy compliance (e.g., granting and revocation of user rights).</p> <p>IS.B.19: Authorization for privileged access should be tightly controlled.</p> <p>IS-WP.II.A.1: Determine whether access to system administrator level is adequately controlled and monitored.</p> <p>OT.B.26: Appropriate access controls and monitoring should be in place between service provider's systems and the institution.</p>

<p>PR.PT-4: Communications and control networks are protected.</p>	<p>AC-4, AC-17, AC-18, CP-8, SC-7</p>	<p>A.13.1.1, A.13.2.1</p>	<p>D3.PC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used.</p> <p>D3.PC.Im.Int.1: The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.</p>	<p>IS.B.33: Typical perimeter controls include firewalls that operate at different network layers, malicious code prevention, outbound filtering, intrusion detection and prevention devices, and controls over infrastructure services such as domain name service (DNS). Institutions internally hosting Internet-accessible services should consider implementing additional firewall components that include application-level screening.</p> <p>IS.WP.I.4.1: Evaluate the appropriateness of technical controls mediating access between security domains.</p> <p>Evaluate the adequacy of security policies and standards relative to physical controls over access to hardware, software, storage media, paper records, and facilities.</p> <p>IS.B.46: Management should establish policies restricting remote access and be aware of all remote-access devices attached to their systems.</p> <p>OPS.B.23: Transmission controls should address both physical and logical risks. In large, complex institutions,</p>
---	---------------------------------------	---------------------------	---	---

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
				<p>management should consider segregating wide area networks (WAN) and local area networks (LAN) segments with firewalls that restrict access as well as the content of inbound and outbound traffic.</p> <p>IS.WP.I.4: Review security policies and standards to ensure that they sufficiently address the following areas when considering the risks identified by the institution ... Network Access - Remote Access Controls (including wireless, virtual private network, modems, and Internet-based).</p> <p>OPS.WP.8.1: Determine whether management has implemented appropriate daily operational controls and processes including ... alignment of telecommunication architecture and process with the strategic plan.</p>

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</p>	<p>AC-4, CM-2, SI-4</p>	<p>A.13.1.1, A.13.2.1</p>	<p>D3.DC.Ev.B.1: A normal network activity baseline is established.</p>	<p>IS.B.77: The behavior-based anomaly detection method creates a statistical profile of normal activity on the host or network. Normal activity generally is measured based on the volume of traffic, protocols in use, and connection patterns between various devices. IS-WP-II-M: Determine whether appropriate detection capabilities exist related to network-related anomalies.</p>
<p>DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.</p>	<p>CA-7, IR-5, SI-4</p>	<p>A.12.4.1</p>	<p>D3.DC.Ev.E.1: A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).</p>	<p>IS.B.83: Because the identification of incidents requires monitoring and management, response centers frequently use SIM tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents. IS.WP.II.G.7: Determine whether appropriate logs are maintained and available to support incident detection and response efforts. IS.B.43: Management has the capability to filter logs for potential security events and provide adequate reporting and alerting capabilities.</p>

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
<p>DE.AE-5: Incident alert thresholds are established.</p>	<p>IR-4, IR-5</p>	<p>A.12.4.1</p>	<p>D5.DR.De.B.1: Alert parameters are set for detecting information security incidents that prompt mitigating actions.</p> <p>D3.DC.An.E.4: Thresholds have been established to determine activity within logs that would warrant management response.</p> <p>D3.DC.An.Int.3: Tools actively monitor security logs for anomalous behavior and alert within established parameters.</p>	<p>IS.B.83: Because the identification of incidents requires monitoring and management, response centers frequently use SIM tools to assist in the data collection, analysis, classification, and reporting of activities related to security incidents.</p> <p>IS.WP.II.G.7: Determine whether appropriate logs are maintained and available to support incident detection and response efforts.</p> <p>IS.B.43: Management has the capability to filter logs for potential security events and provide adequate reporting and alerting capabilities.</p>

CSF Subcategory	NIST 800-53 rev4 ^a	IEC/ISO 27001 ^b	FFIEC CAT v1 ^c	FFIEC IT Exam Handbook Information Security ^d
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	A.12.4.1	D3.DC.An.A.3: A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.	<p>IS.B.73: Financial institutions should gain assurance of the adequacy of their risk mitigation strategy and implementation by monitoring network and host activity to identify policy violations and anomalous behavior.</p> <p>IS.WP.II.M.1: Review security procedures for report monitoring to identify unauthorized or unusual activities.</p> <p>IS.B.77: The behavior-based anomaly detection method creates a statistical profile of normal activity on the host or network. Normal activity generally is measured based on the volume of traffic, protocols in use, and connection patterns between various devices.</p>

- 431 a. Mapping taken from “Framework for Improving Critical Infrastructure Cybersecurity,” NIST, February 12, 2014
- 432 b. Mapping taken from “Framework for Improving Critical Infrastructure Cybersecurity,” NIST, February 12, 2014
- 433 c. Mapping taken from FFIEC Cybersecurity Assessment Tool Appendix B, FFIEC, June 2015
- 434 d. Mapping taken from FFIEC Cybersecurity Assessment Tool Appendix A, FFIEC, June 2015

435 **3.5 Security Functions and Subcategories Related to FFIEC**

436 The example implementation is responsive to the desire to support compliance with the FFIEC CAT
 437 guidance as well as the NIST standards and best practices as detailed in Table 3-1.

438 The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT)
 439 provides specific guidance that applies to financial institutions and was used as a reference by the
 440 development team. The proposed solution is designed to be CAT-informed. This document attempts to
 441 capture some of the key areas where CAT guidance is relevant to elements of the solution and its
 442 implementation, for reference purposes. Please consult an auditor or examiner for any questions on
 443 FFIEC compliance.

444 The example implementation is informed by FFIEC CAT guidance and may contribute to CAT-aligned
 445 implementations by providing mechanisms supporting management, logging, and auditing of all ARM
 446 activity efficiently and cost effectively. With this solution in place, information regarding which users
 447 have access to which resources is maintained by the existing directories and modified via the central
 448 administration and provisioning system. Without the solution, the user access information is provisioned
 449 separately to each directory.

450 Table 3.2 describes how the ARM solution supports compliance with FFIEC CAT guidance.

451 **Table 3-2 FFIEC CAT Guidance**

FFIEC CAT Guidance	ARM Solution Characteristics
D4.C.Co.Int.1: A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.	Data flows into and out of the ARM system are documented and enforced because of the asset value to the organization.
D1.G.IT.B.2: Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.	The ARM system is classified as a critical asset that needs to be protected.
D3.PC.AM.B.6: Identification and authentication are required and managed for access to systems, applications, and hardware.	The ARM system manages the updates to the identity and authentication systems (directories) using automation to ensure access policy compliance.
D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.	The ARM workflow receives information from the HR system on terminations and job changes. It can immediately de-provision access for these employees. The

FFIEC CAT Guidance	ARM Solution Characteristics
	workflow can also include an approval process.
<p>D3.PC.Am.B.15: Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.</p> <p>D3.PC.Im.Int.2: Security controls are used for remote access to all administrative consoles, including restricted virtual systems.</p> <p>D3.PC.Am.B.1: Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.</p> <p>D3.PC.Am.B.2: Employee access to systems and confidential data provides for separation of duties.</p> <p>D3.PC.Am.B.5: Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.</p> <p>D3.PC.Am.Int.1: The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.</p>	<p>A privileged account management (PAM) system is not required as part of an ARM solution. PAM was included to enhance the security of the implementation and addresses this guidance.</p>
<p>D3.PC.Am.B.13: Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).</p> <p>D3.PC.Am.E.5: Controls are in place to prevent unauthorized access to cryptographic keys.</p> <p>D3.PC.Am.Int.7: Confidential data is encrypted in transit across private connections (e.g., frame relay and T1) and within the institution’s trusted zones.</p> <p>D3.PC.Im.B.1: Network perimeter defense tools (e.g., border router and firewall) are used.</p> <p>D3.PC.Im.Int.1: The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air-gapping) to mitigate attacks.</p>	<p>The solution uses Lightweight Directory Access Protocol Secure (LDAPS) to protect data-in-transit between the ARM provisioning system and the directories. The solution is implemented to address this guidance.</p>
<p>D2.MA.Ma.B.1: Audit log records and other security event logs are reviewed and retained in a secure manner.</p>	<p>The ARM solution includes a security management and monitoring system to address this guidance.</p>

FFIEC CAT Guidance	ARM Solution Characteristics
<p>D3.PC.Am.B.4: User access reviews are performed periodically for all systems and applications based on the risk to the application or system.</p> <p>D3.PC.Am.B.3: Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).</p> <p>D4.RM.Om.Int.1: Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.</p> <p>D3.DC.Ev.E.1: A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).</p> <p>D5.DR.De.B.1: Alert parameters are set for detecting information security incidents that prompt mitigating actions.</p> <p>D3.DC.An.E.4: Thresholds have been established to determine activity within logs that would warrant management response.</p> <p>D3.DC.An.Int.3: Tools actively monitor security logs for anomalous behavior and alert within established parameters.</p> <p>D3.DC.An.A.3: A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.</p>	

453 **3.6 Technologies**

454 Table 3.3 lists all the technologies used in this project and provides a mapping between the generic application term, the specific product used,
 455 and the security control(s) that the product provides. (Recall that Table 3-1 explained the CSF subcategory codes.) This table describes only the
 456 product capabilities used in our example solution. Many of the products have additional security capabilities that were not used in our example
 457 implementation. The table's Product column contains links to vendor product information that describes the full capabilities.

458 **Table 3-3 Products and Technologies**

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
Provision, modify or revoke access throughout all user information repositories (directories)	User access policy management	PR.AC-1: Identities and credentials are managed for authorized devices and users.	Virtual Directory	Radiant Logic	RadiantOne VDS Note: Radiant Logic changed their product name from RadiantOne Virtual Directory Server (VDS) to RadiantOne Federated Identity Service (FID)		Consolidated source for digital identities and authorized access to resources
	User access policy management	PR.AC-1: Identities and credentials are managed for authorized	Policy management	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the ARM workflow to Active Directory, OpenLDAP, and Vanguard

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
	User access authoritative information repository	devices and users. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	User access information management	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the ARM workflow to Active Directory, OpenLDAP, and Vanguard
	Centralized provisioning of access information		Provisioning	AlertEnterprise	Guardian	4.0 SP04 HF3	Provisions access authorizations from the ARM workflow to Active Directory, OpenLDAP, and Vanguard
	User access information repository		Directory	AlertEnterprise	Guardian	4.0 SP04 HF3	Maintains the authoritative source for user access information
				Microsoft	Active Directory		User access information repository
			OpenLDAP	OpenLDAP		User access information repository	
			Mainframe RACF interface	Vanguard Integrity Professionals	Vanguard		User access information repository and RACF (mainframe access control interface)

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
	Privileged user access control	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality.	Privileged User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access by privileged users of operating systems (OSs) and applications. Limits functions available to privileged users to reduce the potential of out of policy activities.
		PR.AC-3: Remote access is managed.	Privileged User Access Management	HyTrust	CloudControl		Creates an audit trail of access by privileged users of the virtual environment management system
Protect data	Protect stored data	PR.DS-1: Data-at-rest is protected.	Privileged User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access by privileged users of OSs and applications. Limits functions available to privileged users to reduce the potential of out of policy activities.
	Protect data while in transit	PR.DS-2: Data-in-transit is protected.		Multiple products	-		Data-in-transit is protected using encrypted transmissions such as LDAPS. Protection is also provided via network segmentation.

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
	Limit functions available to privileged users	PR.DS-5: Protections against data leaks are implemented.	Privileged User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access by privileged users of OSs and applications. Limits functions available to privileged users to reduce the potential of out-of-policy activities.
	Limit access to control network	PR.PT-4: Communications and control networks are protected.		Multiple products	-		Communications are protected through network segmentation.
Track privilege user activity	Monitor privileged user activity	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	Log data aggregation, analysis and correlation	Splunk	Enterprise	6.4	Records logs from all systems to monitor for anomalous personnel activity.
			Privileged User Access Management	TDi Technologies	Console Works	4.9-0u0	Creates an audit trail of access by privileged users of OSs and applications. Limits functions available to privileged users to reduce the potential of out of policy activities.

Security Characteristics	Security Capability	CSF Subcategory	Application	Company	Product	Version	Use
Log aggregation, correlation and analysis	Aggregate log data and analyze for anomalous activity	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	Log data aggregation, analysis and correlation	Splunk	Enterprise	6.4	Records logs from all systems to monitor for anomalous personnel activity.
	Generate alerts based on anomalous activity	DE.AE-5: Incident alert thresholds are established.	Log data aggregation, analysis and correlation	Splunk	Enterprise	6.4	Log analysis and correlation rules are established to alert incidents.
	Log management	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	Log data timing and security	TDi Technologies	Console Works	4.9-0u0	Controls access to industrial control system (ICS) devices by people (ICS engineers and technicians).
	Log aggregation and analysis		Log data aggregation, analysis and correlation	Splunk	Enterprise	6.4	Records logs for analysis and correlation.

459

460 4 Architecture

461 ARM involves the organization and control (by organizational policy) of approved access information
 462 (directory user account details) used to authenticate and authorize users for access to organizational
 463 resources. This guide presents an architecture for implementing an ARM automation and security
 464 solution, which improves the control of access information and the cybersecurity monitoring of the
 465 information repositories (directories).

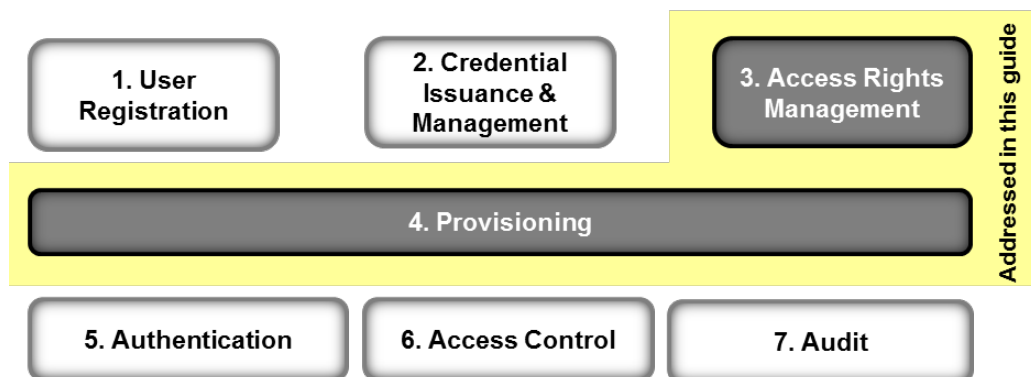
466 This section describes the high-level architecture and reference design for the ARM system.

467 4.1 Architecture Description

468 4.1.1 High-Level Architecture

469 Figure 4-1 depicts a high-level architecture for identity and access management systems, followed by a
 470 description of each of the capabilities. The ARM-solution described in this practice guide is composed of
 471 the capabilities illustrated in the yellow portion of Figure 4-1 and is designed to address the security
 472 functions and subcategories described in Table 3-1.

473 Figure 4-1 ARM High-Level Architecture



474

- 475 1. **User registration** determines that there is a reason to give a person access to resources, verifies
 476 the person's identity, and creates one or more digital identities for the person.
- 477 2. **Credential issuance and management** [3] provides life-cycle management of credentials such as
 478 employee badges or digital certificates.
- 479 3. **Access rights management** (ARM) determines the resources a digital identity is allowed to use.
 480 Arm includes Policy Management and Policy Administration capabilities. (addressed by this
 481 guide). In this document, the terms digital identity, account, and user access information are
 482 synonymous.

- 483 4. **Provisioning** populates repositories (directories) digital identity, credential, and access rights
484 information for use in authentication, access control, and audit. (addressed by this guide).
- 485 5. **Authentication** establishes confidence in a person's digital identity.
- 486 6. **Access control** [4] allows or denies a digital identity access to a resource.
- 487 7. **Audit** maintains a record of resource access attempts by a digital identity as well as changes to
488 digital identities.

489 The following capabilities included in the high-level architecture are not addressed in this practice guide:
490 User Registration, Credential Issuance and Management, Authentication, Access Control and Audit.
491 These capabilities are not addressed because they are either manual administrative processes invoked
492 when an employee is hired or changes jobs or are automated (run-time) activities that occur every time
493 a person attempts to access a corporate resource (e.g., computer system).

494 Access rights management and provisioning are addressed in the project. Provisioning connects the
495 administrative activities to the run-time activities by populating and modifying the directories with the
496 user access information. Access rights management (policy management and administration) includes
497 automated functions such as assigning user access rights based organizational policies and determining
498 the proper user access information to be stored in the directories.

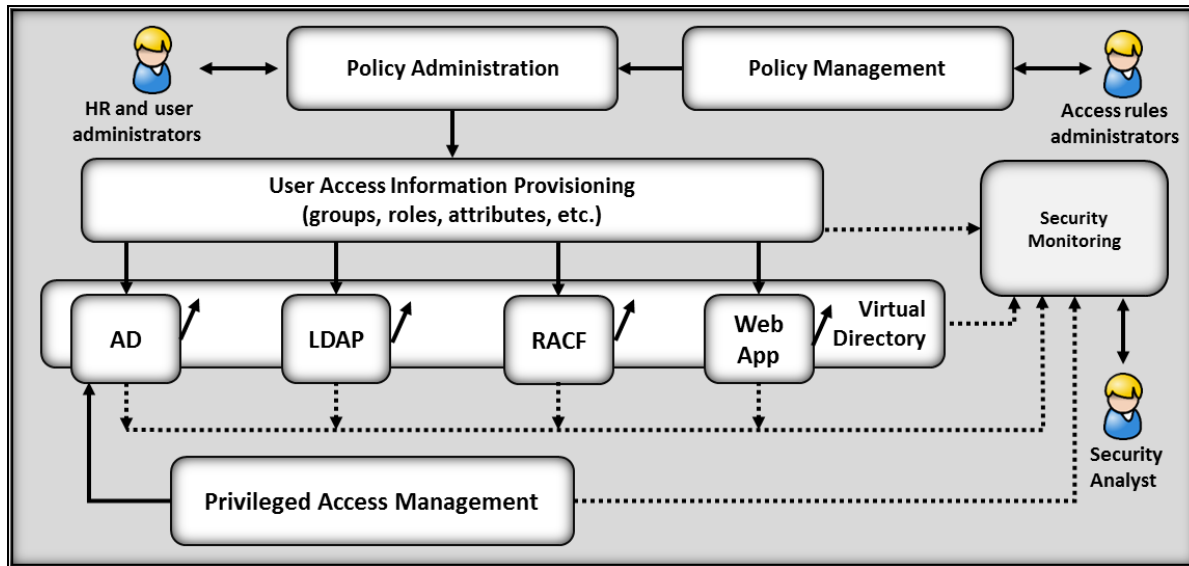
499 Directories, such as Microsoft Active Directory (AD), Resource Access Control Facility (RACF), and
500 OpenLDAP, are often used in the implementation of run-time functions. Companies typically maintain
501 multiple directories based on application needs and business acquisitions/combinations. These
502 directories are often managed by multiple administrators. Managing access information across
503 directories is complicated because of the coordination effort required among directory administrators.
504 This leads to unwanted situations such as:

- 505 ■ administrators finding it difficult to ensure that employees have access to the resources they
506 need to perform their jobs, and only those resources
- 507 ■ newly hired employees not having access to all the resources they need
- 508 ■ employees who change jobs retaining access to resources they no longer need (access or
509 privilege creep)
- 510 ■ terminated employees retaining access long after they leave

511 4.1.2 Reference Design

512 The reference design described here addresses the unwanted situations by implementing ARM and
513 Provisioning capabilities for an enterprise. Figure 4-2 illustrates the reference design of the solution.

514 Figure 4-2 ARM Reference Design



515

516 Note: 1) Solid lines represent policy and user access information transfer/communications, 2) the dotted
 517 lines indicate system event and log transfer/communications.

518 The *Policy Management* capability provides the interface and automation that enable the company to
 519 document and store access policy rules for use by the *Policy Administration* capability. The *Policy*
 520 *Management* system includes an interface for business and application owners to record the attributes,
 521 groups, or roles that are required to allow access to data and applications.

522 For example, an individual who serves in the role of bank manager and works in the mid-west division of
 523 her company may be given certain access rights that are denied to a bank manager in a different region
 524 or division. Implementation of separation of duties and of least privilege access policies enables
 525 organizations to reduce the risk of unauthorized access. However, over time, the number and
 526 combination of attributes, group memberships, and roles can be quite large. Companies should make
 527 efforts to consolidate the attributes, group memberships, and roles used to reduce the number of
 528 combinations and complexity **wherever possible**.

529 The *Policy Administration* capability provides the interface and automation, including approval
 530 workflows, to create, modify, and disable user accounts within the directories. It also provides the
 531 automation to read files from an HR system that contain user information (new, changed, or terminated
 532 employee information). After the *Policy Administration* system reads the user information, it references
 533 the user access policies from the *Policy Management* system and initiates any workflows required for
 534 access approvals. The workflow may require multiple approvals. In some cases, workflows check for
 535 training or other corporate credentials as part of the approval process. The system will then initiate the
 536 approved changes (performed by the provisioning capability) needed in all the directories of the

537 company, virtually simultaneously and within corporate policy. Automation greatly reduces the chances
538 of incorrect account creation or changes.

539 The *User Access Information Provisioning* capability performs the directory access and change functions
540 to apply the approved changes processed by the *Policy Administration* system. The provisioning
541 capability generates logs for each change action. The *Security Monitor* uses these logs as an input to the
542 anomalous activity monitoring analytics.

543 The *Virtual Directory* capability performs a directory caching function that is used to monitor the state of
544 the directories. The *Virtual Directory* is configured to mirror the contents of the directories. Directory
545 changes are identified in real time and logged by the *Virtual Directory*. The *Security Monitor* uses this
546 information as an input to the anomalous activity monitoring analytics.

547 The *Privileged Account Management (PAM)* capability provides the management and control of
548 privileged users of the ARM capabilities and underlying infrastructure. The capability includes logging of
549 user actions (including keystrokes and mouse clicks) and logins, credential management, and user action
550 controls. The *Security Monitor* uses this information as an input to the anomalous activity monitoring
551 analytics. User action controls can include limiting the types of commands users can run.

552 The *Security Monitor* capability collects and analyzes logs from the provisioning capability, directories,
553 PAM, and the virtual directory. Analytics monitor the incoming logs for indications of anomalous activity.
554 In the example implementation, anomalous activity has been defined as any change to a user account
555 within any directory that the provisioning system did not initiate. Analytics have been created to
556 generate an alert for unexpected changes and logins. Unexpected changes may be an indicator of
557 preparations for or actual malicious activity. The Security Monitoring capability also monitors the PAM
558 capability for all system logins. The monitoring analytics will correlate these logins with directory
559 changes.

560 The ARM workflow is a pre-defined sequence of steps to process each user access change request. The
561 steps may include approval requests that require an individual or individuals to acknowledge and
562 approve a user access information change before the workflow completes and the change is
563 provisioned. The ARM capability, through provisioning, manages changes to the information in the
564 directories. The combined capabilities can reduce the time to update access information. They also
565 ensure that changes are provisioned consistently across multiple directories and improve the audit trail.
566 The Monitoring Capability is designed to identify directory changes generated by the provisioning
567 system and approved administrators. If an unauthorized change to the user access information in a
568 directory occurs (i.e., a change is made directly rather than being made via the provisioning system), the
569 monitoring system generates an alert for the security analysts. Once an ARM solution is implemented,

570 administrators do not need to make changes to the directories except for limited situations using the
571 PAM capability.

THE EXAMPLE IMPLEMENTATION WAS DESIGNED TO ADDRESS FOUR BASIC TRANSACTIONS:

1. Creating all required user access information for a new employee in the appropriate directories
2. Updating directories for an existing employee who is changing jobs or requires a temporary access change (or change to contractor status)
3. Disabling all user accounts within ALL the appropriate directories for a terminated employee
4. Improving monitoring of directories for anomalous activity

572 The reference design does not assume that each person will have a single digital identity. A current
573 employee is likely to have several distinct digital identities because of independent management of the
574 directories. Requiring a single digital identity would create a significant challenge to the adoption and
575 implementation of the reference design. The reference design supports continued use of multiple digital
576 identifiers for employees. A virtual directory has been included in the solution to enhance the security of
577 the directories by monitoring them for changes in real time. The virtual directory can also be used to
578 assist in migrating users to a single digital identity.

579 Whereas the system to manage access changes is converged, the authority to make access changes
580 remains distributed among appropriate company management. Some access changes will require
581 explicit approval before being authorized. For these situations, the workflow notifies one or more access
582 approvers for each such resource and waits for responses. When the workflow receives approvals, it
583 provisions the authorized access changes in the directories. All information about approved, pending,
584 and provisioned access changes are maintained in the workflow system. Pending access authorizations
585 may be either authorizations that have been approved but not yet provisioned or time-bounded
586 authorizations to be provisioned/de-provisioned at a future time. Explicit approval is used to ensure that
587 managers and system owners retain control over access to critical systems.

588 When the HR system notifies the workflow that an employee has been terminated, the workflow
589 removes or disables all the employee's accounts from the directories. Integration with HR allows for
590 rapid activation, changes and de-activation of accounts across the organization. These capabilities
591 reduce overhead and administrative downtime. Organizations may benefit significantly from reductions
592 in the time to change access.

593 **5 Example Implementation**

594 This section describes the components of the example implementation of the reference design
 595 described in [Section 4](#). A repeatable, demonstrable example of the reference design, it uses the
 596 products of participating vendors (collaboration team). The example implementation is not a reference
 597 implementation because, we believe, the products used are not the only products (or combination of
 598 products) that can provide the capabilities in the reference design.

599 **5.1 Example Implementation Description**

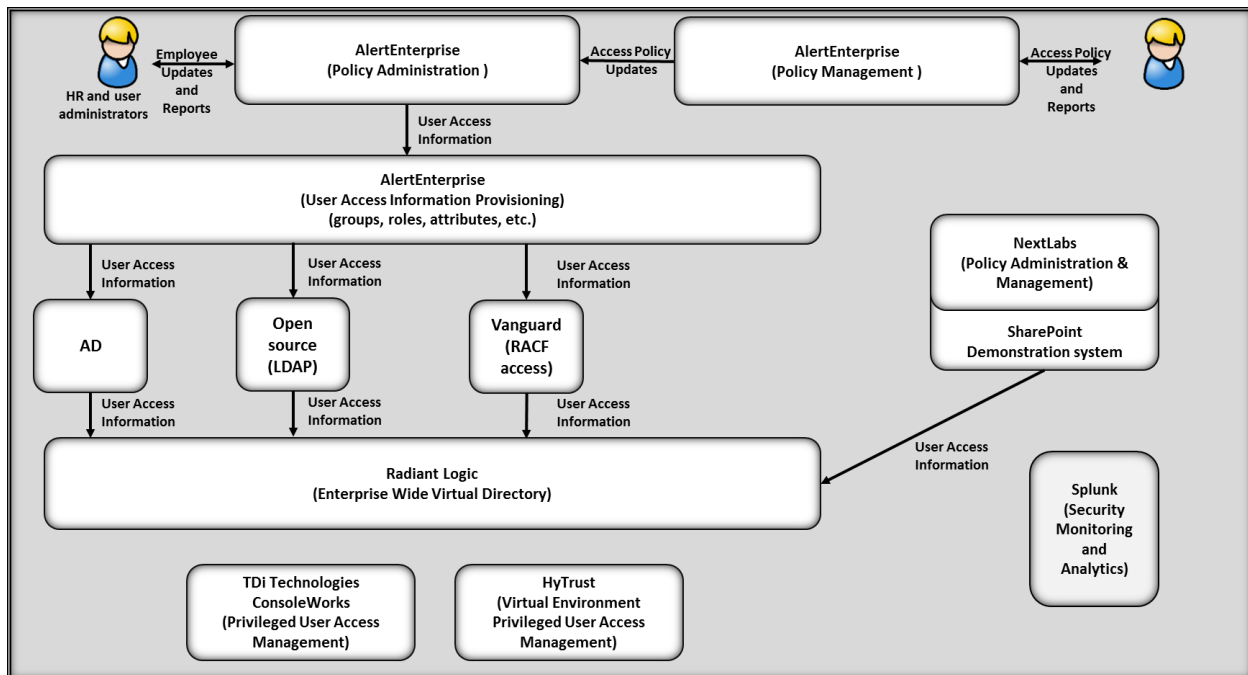
600 The example implementation is constructed on the NCCoE lab's infrastructure, which consists of a
 601 VMware vSphere virtualization operating environment. We used network-attached storage and virtual
 602 switches to interconnect the solution components as well as Internet access. The lab network is not
 603 connected to the NIST enterprise network. Table 5-1 lists (alphabetically) the software and hardware
 604 components we used in the example implementation, as well the specific function each component
 605 contributes.

606 **Table 5-1 Example Implementation Component List**

Product Vendor	Component Name	Function
AlertEnterprise	Enterprise Guardian	Automation, interface and translation between ARM IdAM servers and the HR system
HyTrust	Cloud Control	Privileged user access controller, monitor, and logging system for VSphere
NextLabs	NextLabs	Attribute-based access control interface for SharePoint
Radiant Logic	RadiantOne	Virtual directory system
Splunk	Enterprise	Log aggregation and analytics system
TDi Technologies	ConsoleWorks	Privileged user access controller, monitor, and logging system
Vanguard Integrity Professionals	Vanguard	Mainframe RACF to LDAP interface system

607 Figure 5-1 illustrates the example implementation.

608 Figure 5-1 Example Implementation



609

610 *Note:* The lines indicate the direction of information flow among components of the architecture.

611 AlertEnterprise (AE) Enterprise Guardian implements the workflow (*Policy Administration*) and the *Policy*
 612 *Management* capabilities. It receives input from an HR system, which we simulated using a manually
 613 produced comma-separated value (.csv) file. A .csv file was used to simulate a human resources (HR)
 614 system because the NCCoE lab does not have an HR system. A mutually authenticated, integrity-
 615 protected connection between an HR system and the Policy Administration capability is the preferred
 616 solution. AE Enterprise Guardian also provisions information to the directory instances. No relationship
 617 among these directories is assumed. The Policy Management capability provides an interface for
 618 management to record access/privilege policies.

619 Privileged account management is an important to ensure separation of duties and manage
 620 administrative accesses. ConsoleWorks uses the Active Directory account information to control
 621 privileged user access to OS and application administrative accounts. In addition, we installed HyTrust
 622 Cloud Control, to manage privileged user access to the virtual environment management accounts.
 623 Cloud Control was installed with manually assigned user access permissions to depict an alternative
 624 approach for the implementation of privileged account management.

625 Radiant Logic RadiantOne Virtual Directory System (VDS) is integrated with the directories in the
 626 solution: Active Directory, OpenLDAP, and Vanguard. RadiantOne provides a Virtual Directory capability
 627 that is used to integrate the group and attribute information from each directory for each user into a

628 single view. In the example implementation, the caching capability of this product provides a directory
629 Monitoring capability that identifies user access/account changes in real time and reports those changes
630 to the Security Monitoring capability.

631 NextLabs is integrated with an instance of SharePoint. NextLabs provides an attribute based access
632 control system used in conjunction with the VDS to demonstrate the ARM example implementation
633 functionality.

634 Splunk Enterprise is integrated with the directories, VDS, and Enterprise Guardian provisioning systems.
635 It is used for log aggregation and storage as well for log analytics and correlation to identify anomalous
636 conditions for security event alerting purposes.

637 5.2 Operation of the Example Implementation

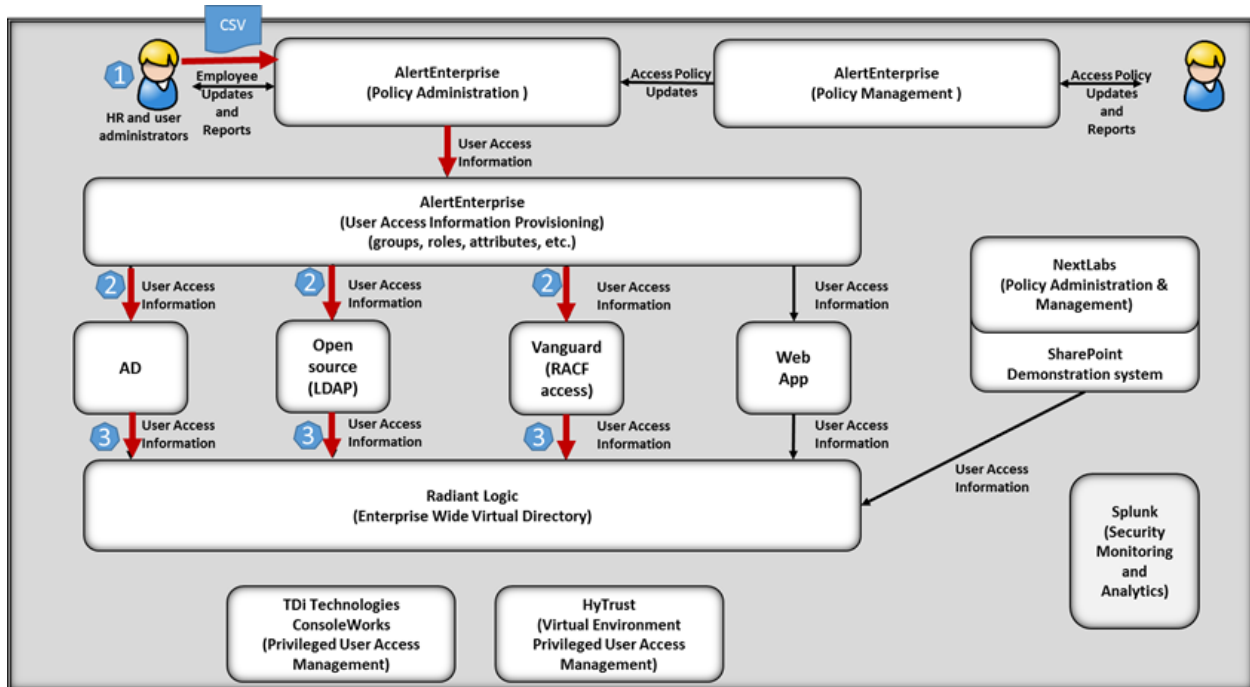
638 This section explains how the example implementation addresses the risk functions identified in [Section](#)
639 [3.4.1](#). Those factors include inability to centrally manage user accounts and inability to provision,
640 modify, or revoke access throughout the enterprise in a timely manner.

641 Before operating the solution, the access policies are recorded in the Policy Management capability. The
642 AE Enterprise Guardian (policy management system) capability assists in automated policy compliance
643 by providing an interface to record enterprise access policies. The policy management system feeds the
644 policy administration system with the policy rules required to assign user access information to
645 employees when new employees join the enterprise or change jobs.

646 The operation of the solution has three primary steps:

- 647 1. An update comes from the HR system (see Figure 5-2). The update consists of a .csv file that
648 contains data on new employees and job changes for existing employees (including terminated
649 employees). The AE Enterprise Guardian (policy administration system) reads the data from the
650 HR .csv file. It then initiates the workflow that identifies the user access information to be
651 provisioned to the appropriate directories based on the policies stored in the Policy
652 Management capability. The example implementation does not include management approval
653 in the workflow.
- 654 2. The workflow passes the user access information to the provisioning system, which populates
655 the appropriate directories with the user/account access information (e.g., group membership,
656 attributes) for new users and makes changes to the information for existing users as needed,
657 based on the HR user update. If an employee is terminated, all his or her accounts are disabled
658 in this step. Data-in-transit is protected using encryption.
- 659 3. once the directories are updated, the updates propagate to the virtual directory. The VDS
660 compares the new version of the directory contents to its cached version at pre-defined
661 intervals. If changes are identified, they are recorded by updating the cache and reported via the
662 logging function. Data-in-transit is protected using encryption.

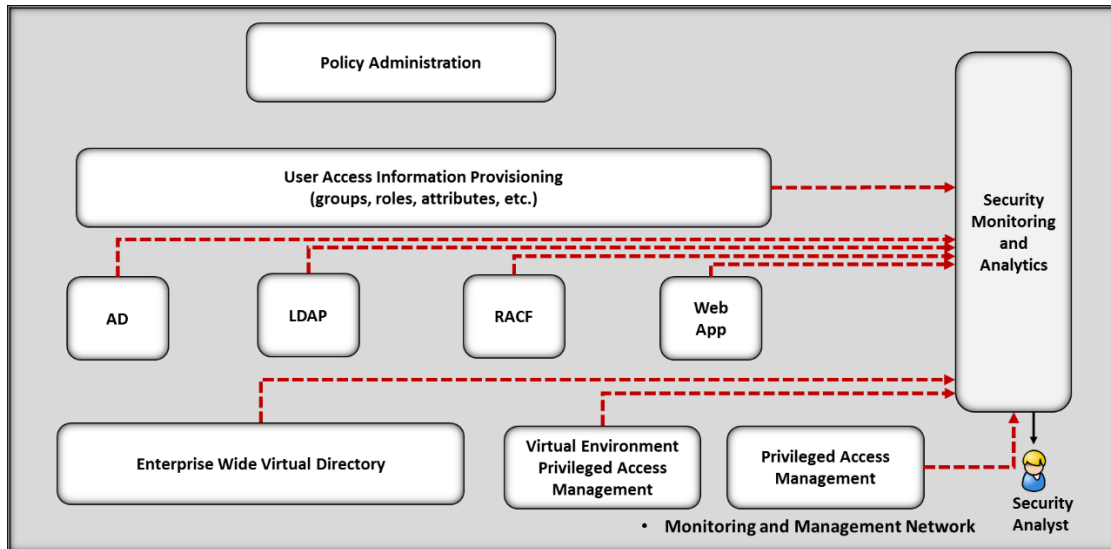
663 Figure 5-2 Example Implementation Data Flow



664

665 *Note:* The red lines show the data flows; their arrows indicate the flow direction.

666 The solution includes a monitoring and analytics component to detect anomalous conditions and activity
 667 (see Figure 5-3). The analytics correlate logs from the provisioning system with logs from the directories
 668 and the virtual directory. The logs from each system report changes to user/account information.
 669 Therefore, all changes to an account within a directory must match the changes reported from the
 670 provisioning system and virtual directory. If changes occur without matching logs, the security
 671 Monitoring Capability generates an alert for an analyst to investigate. The full assessment of the security
 672 aspects of the solution are described in [Section 6](#).

673 **Figure 5-3 Monitoring Data Flow**

674

675 *Note:* The red dashed lines depict data flows with arrows indicating the flow direction. The data in
 676 transit is protected by encryption.

677 Privileged accounts are accessed via the PAM system. These accounts/users have permission to make
 678 changes and maintain the systems within their authority. All use of the PAM system is monitored and
 679 logged by the Security Monitoring Capability. Anomalous activity for a privileged account, including
 680 multiple failed PAM system login attempts, can be configured to alert.

681 The NextLabs system is used in conjunction with SharePoint to demonstrate the ARM example
 682 implementation operations. NextLabs integrates with SharePoint to manage access to SharePoint
 683 pages/sites. In the example implementation, SharePoint represents web applications. The site access is
 684 based on an attribute-based access control model implemented in the NextLabs system. NextLabs
 685 provides the policy decision point capability for the demonstration. NextLabs uses the VDS for user
 686 access information.

687 5.2.1 Example Implementation Network Components Overview

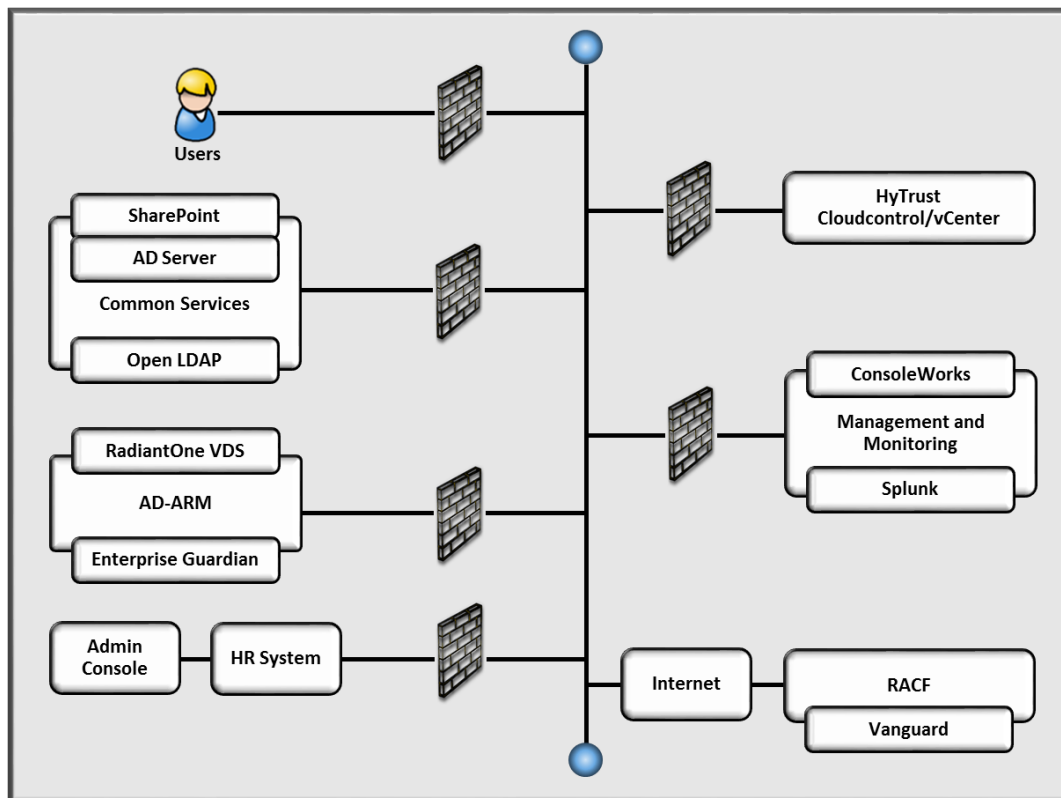
688 The example implementation architecture consists of multiple networks that partially mirror the
 689 infrastructure of a typical financial services company. A management network was implemented to
 690 facilitate the management and monitoring of the systems. The example implementation consists of the
 691 following subnetworks:

- 692 ▪ common services
- 693 ▪ access rights management (ID-ARM)
- 694 ▪ end-user systems

- 695 ▪ virtual environment management
- 696 ▪ users
- 697 ▪ management and monitoring
- 698 ▪ HR
- 699 ▪ backbone

700 These subnetworks were implemented separately in line with best practices for enterprise
701 infrastructure. Firewalls block all traffic except required internet communications.

702 **Figure 5-4 ARM Example Implementation Network**



703

704 The subnetworks shown in Figure 5-4 are described in the following paragraphs.

705 **Internet**—The lab environment can access the public Internet to facilitate access to a mainframe (RACF)
706 Vanguard Authenticator demonstration system (provided by Vanguard Integrity Professionals) by the
707 ARM example implementation.

708 **Switching and Routing**—Switching in the architecture is executed using a series of physical and virtual
709 switches. Virtual Local Area Networks (VLANs) are implemented to segment the networks shown in

710 Figure 5-4. VLAN switching functions are handled by physical switches and the virtual environment.
 711 Routing was accomplished using routers that also hosted the firewalls.

712 **Backbone**—The backbone network provides a protected network space that the other networks can use
 713 to route traffic across.

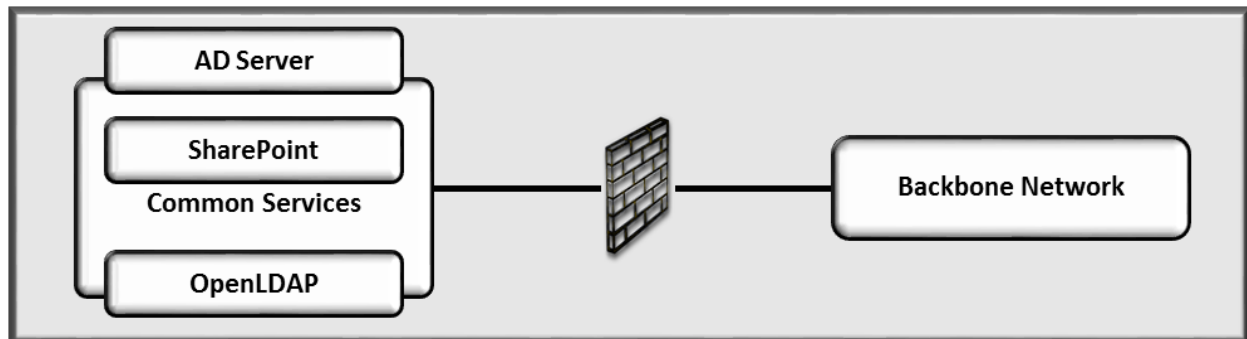
714 5.2.2 Common Services Network

715 The example implementation includes the following common services components:

- 716 ▪ Active Directory
- 717 ▪ OpenLDAP directory
- 718 ▪ SharePoint servers

719 A typical enterprise includes other shared services, such as email servers. We did not include these in
 720 the architecture because they are not needed to demonstrate the effectiveness of the ARM example
 721 implementation. Table 5-1 and Figure 5-5 identify the specific vendor products we used in this network.

722 **Figure 5-5 Common Services Network**



723

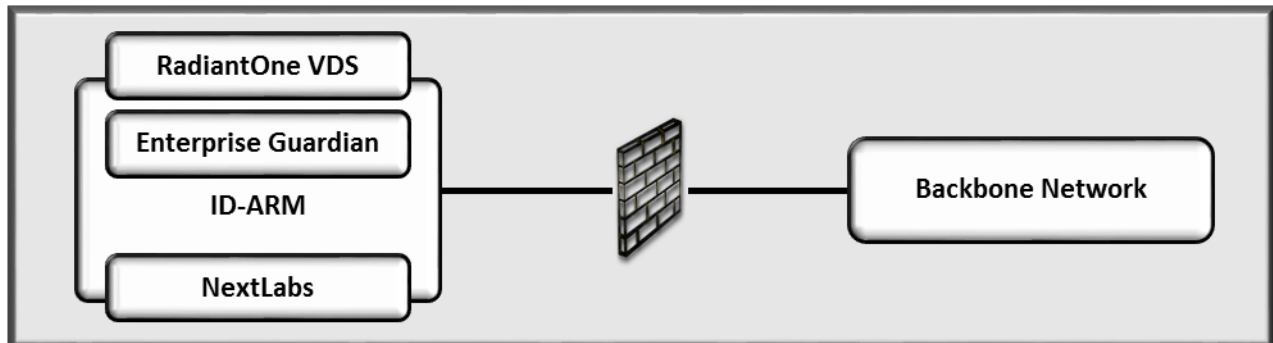
724 5.2.3 Access Rights Management Network

725 The following products were installed on the ARM network

- 726 ▪ AlertEnterprise Enterprise Guardian ARM system
- 727 ▪ Radiant Logic RadiantOne Virtual Directory
- 728 ▪ NextLabs Entitlement Management

729 We separated the ARM systems to highlight the unique ARM components proposed to address the use
 730 case. We do not recommend separating ARM functions on their own network. Organizations need to
 731 determine the most appropriate implementation of an ARM product within their own infrastructure.
 732 Table 5-1 and Figure 5-6 identify the products used in this example implementation.

733 Figure 5-6 ID-ARM Network



734

735 AE Enterprise Guardian provides the workflow management capability. The ARM example
 736 implementation takes over control of the directories in the company. An important aspect of the
 737 implementation is that the control is implemented by assigning an administrative account credential for
 738 each managed directory to the ARM system. When the administrative credential is issued, the company
 739 must limit access to the managed directories to administrative users with a PAM system. The security of
 740 the solution partially depends on limited access to the managed directories, as discussed in [Section 6](#).

741 In this example implementation, the central ARM system uses LDAPS to access and update directories.
 742 This encrypted data-in-transit version of LDAP prevents network sniffers from recording the provisioned
 743 changes. In addition, Radiant Logic's virtual directory product synchronizes with the directories using the
 744 same LDAPS protocol.

745 The Radiant Logic RadiantOne product provides a Virtual Directory capability. In the solution, this
 746 product provides two functions: virtual directory for NextLab's use and directory caching for security
 747 monitoring. This synchronization is set up to identify and record, at pre-defined intervals, changes within
 748 each directory. Radiant Logic reports all changes via logs to the Security Monitoring System.

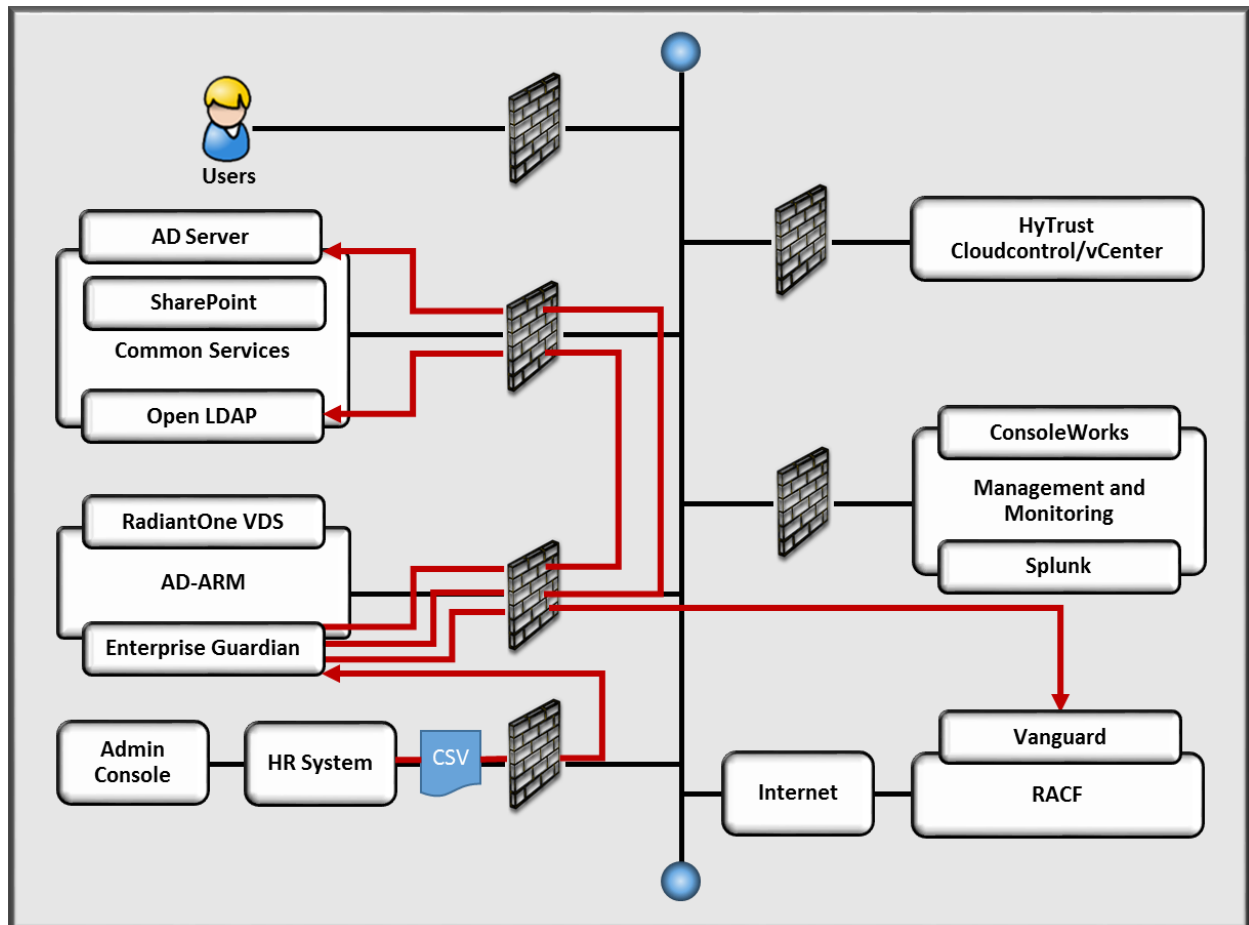
749 The NextLabs Entitlement Management product provides the attribute-based access control capability
 750 for an instance of SharePoint. The NextLabs product provides the policy decisions for SharePoint when
 751 determining access rights for any user attempting to log in to a SharePoint site. This functionality is used
 752 in the demonstration of the example implementation.

753 5.2.4 Network Data Flows

754 This section describes the data flows within the networks implemented in the example implementation.
 755 Figures 5-7 and 5-8 depict data flows using red lines with arrows indicating the flow direction
 756 superimposed on network diagrams. The steps are described in [Section 5.1](#). Figure 5-7 depicts the flow
 757 of user access information from the HR system to the Policy Administration and Provisioning systems
 758 and into the directories. Figure 5-8 depicts the flow of user access information from the directories to

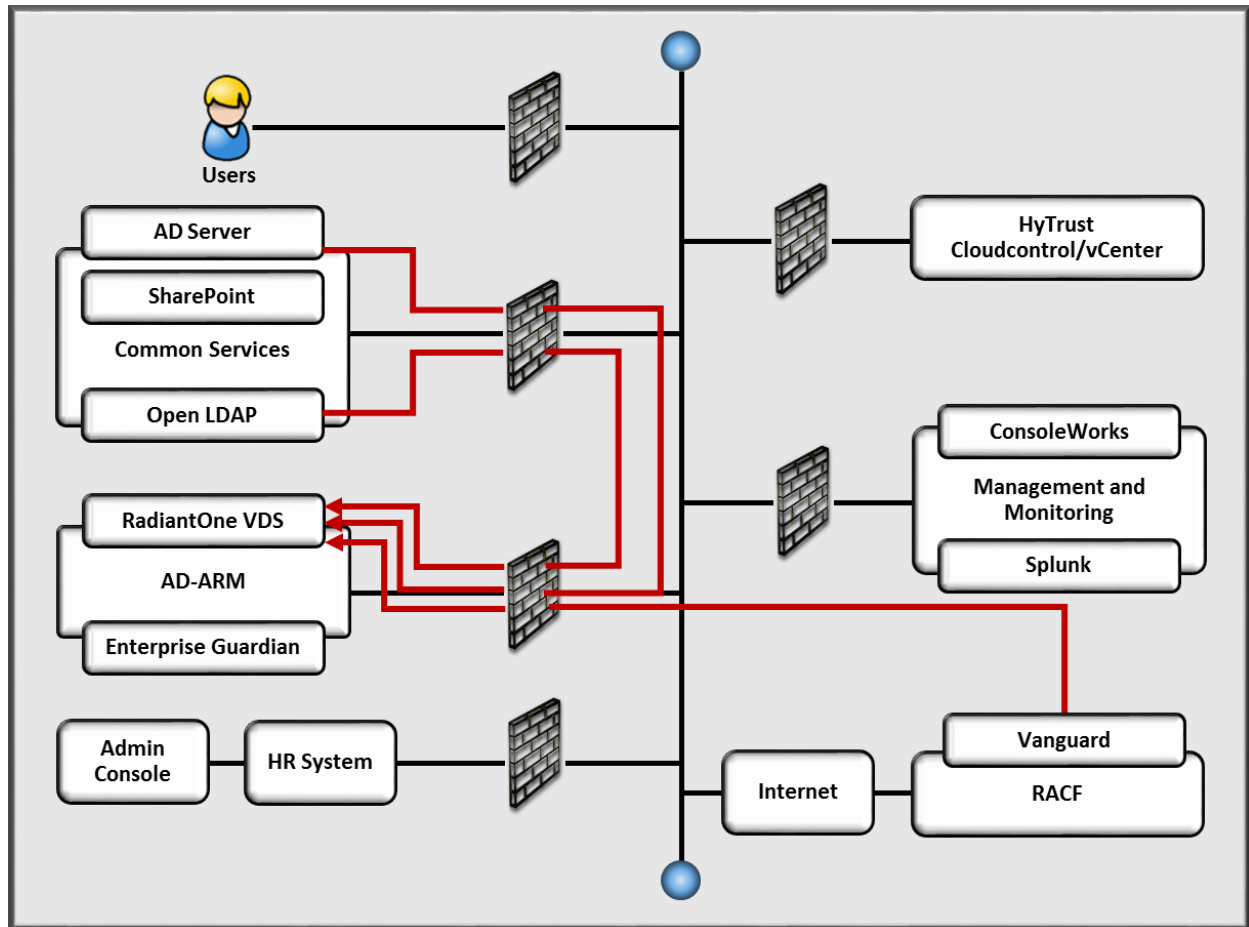
759 the VDS. Note that all data is routed among the ARM and shared services systems through the backbone
760 network. The data-in-transit is protected using LDAPS.

761 **Figure 5-7 User Access Information Network Data Flow (Steps 1 and 2 in Figure 5-2)**



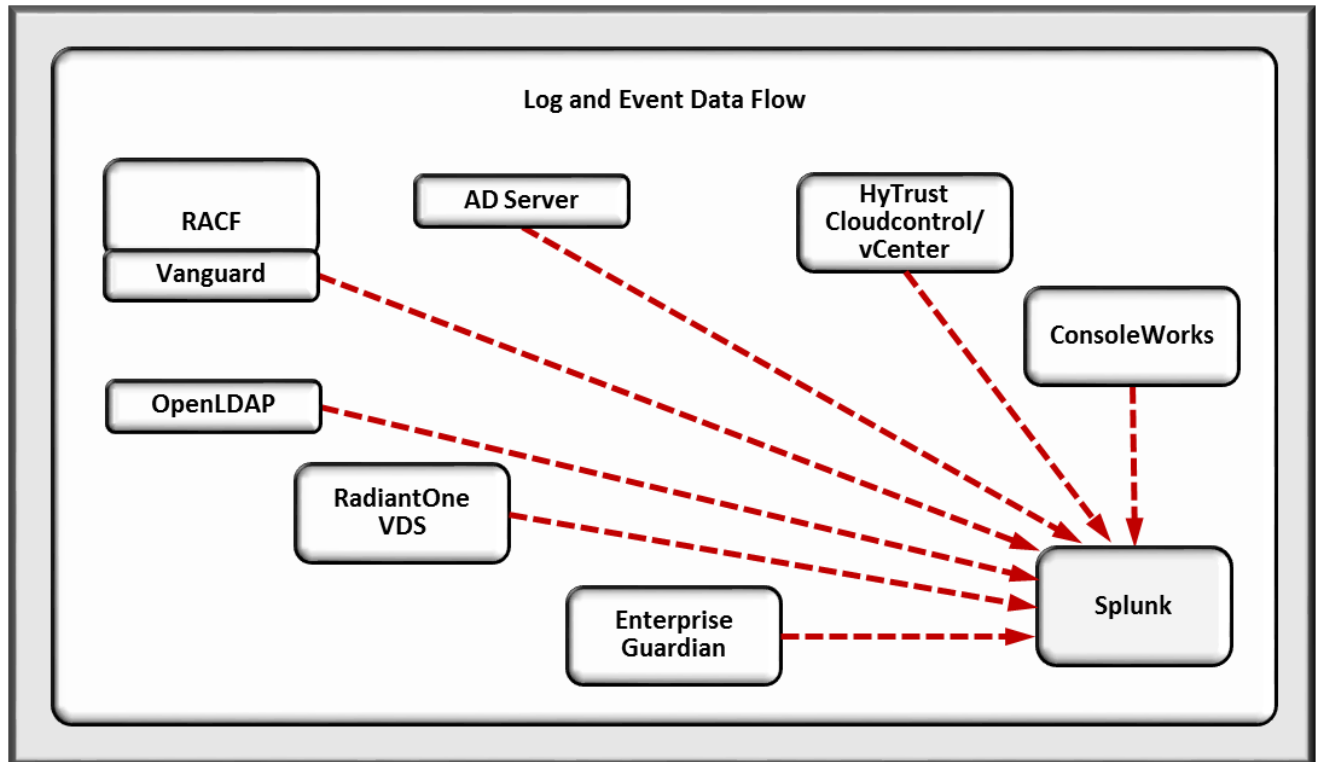
762

763 Figure 5-8 User Access Information Network Data Flow (Step 3 in Figure 5-2)



764
765 The system monitoring data (log and event data) flow occurs between each system and the security
766 monitoring system. Figure 5-9 depicts the data flows. All monitoring and management data are sent via
767 a separate management network segregated from the Backbone (production) network.

768 Figure 5-9 Monitoring Network Data Flow



769

770 *Note:* The red dashed lines depict data flows with arrows indicating the flow direction. The data-in-
 771 transit is protected by encryption.

772 5.3 Data

773 The example implementation requires user dataset files (HR files) in a format similar to that typically
 774 provided by human resource systems. Initially, we populated the HR file with user data from a synthetic
 775 dataset designed to mirror a typical HR system dataset. We used a .csv file, which is a typical HR system
 776 export file type. The data included user names, titles, access assignments, unique identifiers, and other
 777 details required to complete valid directory entries. Each directory was pre-configured with the group
 778 and attribute fields needed to support the example implementation. The details are included in NIST SP
 779 1800-9C: *How-To Guide*.

780 **6 Security Analysis**

781 We organized the security analysis of the ARM reference design into three parts.

- 782 ▪ [Section 6.4, Analysis of the Reference Design’s Support for CSF](#) Subcategories, analyzes the
783 reference design in terms of the specific subcategories of the CSF that it supports. It identifies
784 the security benefits of each of the reference design capabilities and discusses how the
785 reference design supports specific cybersecurity activities, as specified in terms of CSF
786 subcategories.
- 787 ▪ [Section 6.5, Analysis of the Security of the Reference Design](#), reviews vulnerabilities and attack
788 vectors that the reference design might introduce, as well as ways to mitigate them.
- 789 ▪ [Section 6.6, Security Evaluation Summary](#), highlights the results of the security assessment and
790 the recommendations from Sections 6.4 and 6.5.

791 **6.1 Assumptions and Limitations**

792 The security evaluation has the following limitations:

- 793 ▪ It is not a comprehensive test of all security capabilities, nor is it a red team exercise.
- 794 ▪ It cannot identify all weaknesses.
- 795 ▪ It does not include the lab infrastructure. It is assumed that devices are hardened. Testing these
796 devices would reveal only weaknesses in implementation that would not be relevant to those
797 adopting this reference architecture.

798 **6.2 Build Testing**

799 The purpose of the security analysis is to understand the extent to which the example solution meets its
800 objective of demonstrating access rights management functionality as defined in [Section 3.2](#). In
801 addition, it seeks to understand the security benefits and drawbacks of the reference design.

802 **6.3 Scenarios and Findings**

803 As we performed our security analysis, we assessed how well the reference design addresses the CSF
804 subcategories it was intended to support. We used the CSF subcategories to structure the security
805 assessment by consulting the specific sections of each standard cited for that subcategory. The cited
806 sections describe the functions and controls the example implementation would be expected to include
807 and perform. Using the CSF subcategories as a basis for organizing our analysis allowed us to
808 systematically consider how well the reference design supports the intended security functions and
809 controls.

810 **6.4 Analysis of the Reference Design’s Support for CSF Subcategories**

811 Table 6-1, ARM Reference Design Capabilities and Supported CSF Subcategories, lists reference design
812 capabilities, their functions, and the addressed subcategories, along with the products that we used to
813 instantiate each capability in the example implementation. The security evaluation does not focus on
814 these specific products but on the CSF subcategories because, in theory, any number of commercially
815 available products could be substituted to provide the CSF support represented by a given reference
816 design capability.

817 The CSF subcategories column of Table 6-1 lists the CSF subcategories that each capability of the
818 reference design supports. The references provide solution validation points in that they list specific
819 security functions and controls that a solution supporting the desired CSF would include. Using the CSF
820 subcategories as a basis for organizing our analysis allowed us to systematically consider how well the
821 reference design supports specific security activities and provides structure to our security analysis. The
822 remainder of this subsection discusses how the reference design supports each of the identified CSF
823 subcategories.

824 Table 6-1 ARM Reference Design Capabilities and Supported CSF Subcategories

Capability	Specific Product	Function	CSF Subcategories
Policy Management	AlertEnterprise Enterprise Guardian and NextLabs Entitlement Management	Stores access control policy rules as defined by administrators and delivers these rules to the Policy Administration capability. The access control policy rules define which users, roles, and groups have access to which enterprise resources, while also delivering access policy reports to administrators.	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.
Policy Administration	AlertEnterprise Enterprise Guardian and NextLabs Entitlement Management	Manages user access-related attributes (e.g., identities, roles, groups) as specified by input from HR administrators. Combines these user access attributes with the access control policy rules that the Policy Management capability delivers to administer enterprise access policy (i.e., to determine which users, roles, and groups have access to which enterprise resources).	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.
User Access Information Provisioning	AlertEnterprise Enterprise Guardian	Automatically translates the enterprise access policy information that the Policy Administration capability delivers into the corresponding role, attribute, and other parameter values that need to be configured in each individual directory. In this way, the capability automatically provisions to all the directories based on the access information from this single, centralized location. LDAPS is employed to maintain confidentiality and integrity. Also, sends logs of all provisioning activity to the monitoring capability.	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.DS-2: Data-in-transit is protected.

Capability	Specific Product	Function	CSF Subcategories
<p>User Access Information Repository (also referred to as Directory)</p>	<p>Active Directory OpenLDAP Vanguard</p>	<p>Authoritative source for enterprise user identifiers and their associated roles and attributes. Organizations typically use several different such directories; the reference design integrates with each. These directories support access control to specific enterprise resources based on the user access (account) information stored in them. Each time a user access attempt is made, one or more of these directories is consulted and its contents are used to determine whether the access request will be granted. The directories also send logs of every change that is made to their user access (account) information contents to the monitoring capability. LDAPS is employed to maintain confidentiality and integrity.</p>	<p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.DS-2: Data-in-transit is protected. DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</p>
<p>RACF Interface</p>	<p>Vanguard</p>	<p>Interface capability that translates between the RACF system to/from LDAP or LDAPS. The capability enables RACF to interface with both the User Access Information Provisioning capability and the Enterprise-wide Virtual Directory capability using LDAP or LDAPS.</p>	<p>PR.DS-2: Data-in-transit is protected. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.</p>

Capability	Specific Product	Function	CSF Subcategories
<p>Enterprise-wide Virtual Directory</p>	<p>RadiantOne VDS</p>	<p>Virtual Directory containing the aggregation of user access information from each of the several different directories in the reference design. It correlates and disambiguates different user accounts that may exist in various directories to create unique user identities and aggregate all the attributes that each user has in each of the directories. It provides a second, global view of the enterprise’s access control information, in addition to the authoritative copy of user access information that is stored across the several different physical directories. It also sends logs of every change that is made to any user access information to the monitoring capability. LDAPS is employed to maintain confidentiality and integrity. Logs are reported to the monitoring capability.</p>	<p>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.DS-2: Data-in-transit is protected.</p>

Capability	Specific Product	Function	CSF Subcategories
Security Monitoring and Analytics (also referred to as Monitoring)	Splunk Enterprise	Receives security monitoring logs documenting all changes made to user access control and policy information at the User Access Information Provisioning capability, each of the directories, the Virtual Directory, the Privileged Access Management Capability, and the Virtual Environment Privileged Access Management capability. Performs analytics on the logs to detect potential inconsistencies and anomalies that might signal security concerns.	PR.DS-1: Data-at-rest is protected. PR.DS-2: Data-in-transit is protected. PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors. DE.AE-5: Incident alert thresholds are established.

825 *Note:* Table 6-1 describes only the product capabilities and CSF subcategory support that the reference architecture uses. Many of the products
 826 have additional security capabilities that are not listed here.

827 6.4.1 Supported CSF Subcategories

828 The reference design was created to identify a set of capabilities and their relationship to provide an
829 ARM solution. The CSF includes functions, categories, and subcategories that define the capabilities and
830 processes needed to implement a cybersecurity program. Within this practice guide, the NCCoE has
831 identified the CSF subcategory capabilities and processes in Table 3-1 that are desirable to implement an
832 ARM solution. Each of the following sections describes how the ARM reference design addresses the CSF
833 subcategories, included in Table 3-1, with technical capabilities. Also included are the CSF subcategory
834 processes from Table 3-1 that are beyond the scope of the ARM solution but are important for
835 organizations to address. Some CSF subcategories are supported by individual capabilities of the
836 reference design; others, by the reference design as a whole. Yet other CSF subcategories are relevant
837 because the reference design is predicated on their being addressed by the enterprise-wide
838 architecture.

839 6.4.1.1 *ID.AM-3: Organizational communication and data flows are mapped*

840 The reference design:

- 841 ▪ Defines and identifies all ARM-related organizational communication and data flows.
- 842 ▪ Defines each of the directories, as well as the flow of data and connectivity between these
843 directories and other capabilities in the reference design.
- 844 ▪ Supports CSF subcategory ID.AM-3 with respect to access control management information.
- 845 ▪ Does *not* address organizational communication and data flows for any other types of
846 information because they are unique to each organization.

847 By adopting the reference design, an organization thereby fulfills its support for CSF subcategory ID.AM-
848 3 with respect to organizational communication and data flows that are related to access control
849 management.

850 6.4.1.2 *ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-* 851 *party stakeholders are established*

852 The reference design is predicated on there being a clearly defined set of roles and responsibilities for
853 each user that determines that user's access control information (i.e., the roles, groups, and attributes
854 that apply to that user and that thereby determine what resources he or she is authorized to access and
855 at what level of privilege). The organizational access policy administrators define the roles and
856 responsibilities of the entire workforce and describe these roles and responsibilities in terms of which
857 employees have access to what resources (and at what level). They then populate this information into
858 the Policy Management and Policy Administration capabilities of the reference design so it can
859 automatically provision the user access information directories based on the roles and responsibilities
860 that any given company will have defined for the workforce. Once these roles and responsibilities have

861 been established and provided to the reference design, the design then serves as the mechanism for
862 enforcing the access control-related aspects of these roles and responsibilities.

863 The design does not include a capability that audits the user access information within the directories.
864 The NCCoE determined that auditing of directory content was out of scope because the capability is well
865 understood and widely adopted.

866 *6.4.1.3 ID.BE-4: Dependencies and critical functions for delivery of critical services are* 867 *established*

868 With respect to the delivery of the critical service of access control, the reference design establishes the
869 User Access Information Provisioning capability as a centralized source for managing and provisioning all
870 user access control information, and it recognizes this capability as a new critical asset. It also recognizes
871 the importance of each individual directory for storing authoritative user access information and
872 supporting access control, identifying these directories as part of the critical infrastructure. The VDS and
873 the Monitoring Capability are essential for ensuring the integrity of the information the directories
874 store.

875 *6.4.1.4 PR.AC-1: Identities and credentials are managed for authorized devices and users*

876 Managing identities and credentials for authorized devices and users is inherent in and fundamental to
877 the reference design. The objective of the design is to automate administering and provisioning user
878 access changes throughout the enterprise for access control purposes.

879 *6.4.1.5 PR.AC-3: Remote access is managed*

880 To provide security to the reference design capabilities, the reference design does not permit any users,
881 even privileged ones, to log in to the consoles of any reference design capabilities directly. It forces all
882 console access to be performed via PAM systems for physical and virtual machines. In the reference
883 design, PAM enables remote access to the capabilities, managing and logging privileged access to the
884 consoles of physical reference design capabilities. Privileged access to virtual machines is managed by
885 the Virtual Environment (VE) PAM capability. [Section 6.5.3](#) discusses privileged access further.

886 *6.4.1.6 PR.AC-4: Access permissions are managed, incorporating the principles of least* 887 *privilege and separation of duties*

888 The main objective of the reference design is to manage access permissions for all enterprise resources
889 and servers in a converged and automated fashion capable of supporting the principles of least privilege
890 and separation of duties. Once corporate access policies have been defined and integrated with the
891 reference design in the form of access policy updates, access information updates, and enterprise
892 business rules/workflows, the reference design automatically and consistently provisions all the
893 enterprise directories with the access information necessary to ensure that the directories enforce
894 corporate access policies.

895 Access Rules administrators should base corporate access policies on the principles of least privilege and
896 separation of duties. The principle of least privilege, defined as providing the least amount of access (to
897 systems or data) necessary for the user to complete his or her job, and the principle of separation of
898 duties, which restricts the amount of responsibilities held by any one individual, are important security
899 tools. These tools help prevent fraud and abuse by limiting the amount of privilege that individual users
900 have and requiring multiple individuals to collude to accomplish certain goals. The reference design,
901 through its Policy Management, Policy Administration, and User Access Information Provisioning
902 capabilities, ensures that the directories are provisioned based on these enterprise access policies. So,
903 assuming access policies are designed to incorporate the principles of least privilege and separation of
904 duties, the reference design will manage and enforce access permissions according to these principles.

905 In addition, to ensure the security of the reference design itself, typical enterprise users must not be
906 authorized to create or modify user accounts on any enterprise machines. Nor should they be able to log
907 in to any reference design capabilities. Only privileged users should be permitted to access reference
908 design capabilities and the machines on which reference design capabilities run. Various levels of
909 administrator privileges should be established and managed to administer the reference design
910 capabilities themselves and the physical and virtual infrastructure on which the reference capabilities
911 run. All privileged administrative activity must be performed through the PAM and VE PAM capabilities
912 to ensure that all such activity is logged, with the logs being sent from the PAM and VE PAM to the
913 Monitoring Capability for scrutiny. Still higher levels of administrator privileges must be established to
914 administer the PAM and VE PAM capabilities themselves because PAM and VE PAM administrators have
915 the authority to turn off logging and modify the privileges that administrators of other reference design
916 capabilities have. [Section 6.5.3](#) discusses privileged access management and the hierarchy of privileged
917 users in more detail.

918 *6.4.1.7 PR.DS-1: Data-at-rest is protected*

919 User access information is not encrypted while stored at rest. However, this data is spread across the
920 directories, and these directories are in their own security enclave. The security enclave consists of the
921 physical directories only, without any other reference design capabilities, situated on their own
922 subnetwork that is separated from the rest of the reference design by a firewall. The firewall is
923 configured to permit communications using only the specific ports and protocols that are required.

924 Furthermore, although this information is not integrity protected while at rest, its integrity is monitored
925 by the Monitoring capability. The Monitoring capability receives logs of user access information changes
926 from the User Access Information Provisioning and VDS capabilities as well as each of the directories.
927 The Monitoring capability correlates and compares the log information it receives from each of the
928 above capabilities to ensure that the information is consistent across all sources. In this way, it is
929 possible to verify that each change made to the directories is the result of a legitimate, corresponding
930 event at the User Access Information Provisioning capability that resulted from input from the Policy
931 Administration capability. If a change is detected to a directory that cannot be correlated with logs

932 signaling related events at these other capabilities, the Monitoring system generates an alert to signal
933 that this change to the data-at-rest in the directory might be unauthorized. File integrity tools are
934 available to monitor for loss-of-integrity events within systems like directories. These tools are not
935 addressed in the reference design.

936 *6.4.1.8 PR.DS-2: Data-in-transit is protected*

937 LDAPS is used to encrypt user access information while it is in transit between reference design
938 capabilities. In the example implementation, a single application is used to implement the Policy
939 Management, Policy Administration, and User Access Information Provisioning capabilities so that all
940 information flows between these capabilities remain inside the same application and are not
941 transmitted over a network where they would be vulnerable to eavesdropping or tampering. If the
942 reference design were to be built using separate physical components to instantiate the Policy
943 Management, Policy Administration, and User Access Information Provisioning capabilities, messages
944 exchanged among these capabilities would need to be provided with at least data integrity and
945 preferably confidentiality protections. The User Access Information Provisioning capabilities encrypt all
946 logs that they send to the Monitoring Capability. It would thus be very difficult to fake a log from one of
947 these capabilities to the Monitoring capability with the aim of trying to trick the Monitoring capability
948 into thinking that an unauthorized user is permitted to have access. Spoofing such a log would require
949 that an adversary possess the keys used to encrypt the logs.

950 In the current example implementation (RFC 2830), LDAPS is used to perform read-and-write access to
951 the directories and to the VDS capability, ensuring that user access information sent across a network to
952 these remote capabilities is encrypted.

953 Also, when log information is sent to the Monitoring capability, it is encrypted using the Splunk
954 connector application, resulting in protection from disclosure as well as unauthorized modification.

955 *6.4.1.9 PR.DS-5: Protections against data leaks are implemented*

956 The reference design itself, through its focus on management of access permissions, protects the
957 enterprise in general against data leaks that might occur were someone to gain unauthorized access to
958 resources on the production network. By preventing unauthorized access to information, the reference
959 design protects against leaks of that information. The reference design, however, is not intended to
960 protect against exfiltration of information by an authorized user; addressing such an insider threat is not
961 within the scope of the guide. The reference design does, however, include some mechanisms to deter
962 data leaks perpetrated by insiders. The fact that data flows within the reference design are encrypted
963 serves to ensure that even if data-in-transit within the reference design were to be exfiltrated, this
964 information would not be in plaintext form. Also, the PAM capability serves to limit which data
965 privileged users can access, thereby limiting what privileged insiders can exfiltrate and copy. For
966 example, administrators may be given access to administration and configuration directories and not to
967 directories that contain sensitive data files. The PAM capability also logs all privileged user access,

968 ensuring that if a privileged user misuses his or her authority and leaks data, this activity would be
969 recorded in log files.

970 *6.4.1.10 PR.PT-1: Audit/log records are determined, documented, implemented, and*
971 *reviewed in accordance with policy*

972 Although it does not include an audit solution, the reference design supports auditing by aggregating all
973 access-related log information in one location (the Security Monitoring capability), thereby enabling
974 centralized accountability and tracking of access change activity. Locally, various events are monitored
975 and logged at each reference design capability (see NIST SP 1800-9C: *How-To Guides* for a list of events
976 logged). These logs are sent to the Security Monitoring capability. Security Analysts will typically be
977 authorized to have read-only access to these logs to review and respond to potential security events.
978 Monitoring and analytics tools will also have access to these logs for anomaly and potential security
979 event detection. All system administrators or other privileged users are required to use the PAM system.
980 Therefore, any actions they take, including abuse of their privileged access, will be monitored and
981 logged. These logs will be sent to the Security Monitoring capability. Given that access to the logs in the
982 Security Monitoring capability would enable an adversary to delete or modify logs that document
983 adversarial activity, the ability to delete or modify such logs should, by policy, require the cooperation of
984 multiple individuals.

985 *6.4.1.11 PR.PT-3: Access to systems and assets is controlled, incorporating the principle of*
986 *least functionality*

987 The reference design itself, through its focus on managing access permissions, inherently supports the
988 control of access to all enterprise systems and assets. User access information, combined with access
989 policies, can be configured to enforce the principle of least functionality.

990 *6.4.1.12 PR.PT-4: Communications and control networks are protected*

991 Network perimeter defense tools, including border routers and firewalls, are used in the reference
992 design; the directories are isolated on their own subnetwork, separated from the rest of the reference
993 design by a firewall that is configured to permit only ports and protocols required to store and retrieve
994 user access information.

995 Similarly, other capabilities of the reference design are isolated on their own subnetworks, as shown in
996 Section 5. For example, the Security Monitoring capability and PAM are isolated on their own
997 subnetwork, the Policy Administration, Policy Management, User Access Information Provisioning, and
998 VDS capabilities are isolated on their own subnetwork, and the VE PAM is isolated on its own
999 subnetwork. Such separation ensures that if an intruder can gain access to one of these subnetworks,
1000 the resulting access does not provide the opportunity to eavesdrop on traffic that is being exchanged
1001 between reference design capabilities on other networks. Nor can the intruder use a capability on which
1002 he or she has gained a foothold in one subnetwork as a platform from which to launch an attack on

1003 capabilities in another subnetwork if such an attack would require the use of ports or protocols that the
1004 subnetwork's firewall is configured to block.

1005 A management subnetwork is implemented to segment log and administrator access to capabilities. This
1006 segmentation further isolates administrative and log data to reduce the potential of eavesdropping and
1007 rogue user access to administration interfaces.

1008 *6.4.1.13 DE.AE-1: A baseline of network operations and expected data flows for users and*
1009 *systems is established and managed*

1010 Within the reference design, the directories constitute the authoritative repositories of user access
1011 information (accounts). The contents of these directories can be considered the baseline with respect to
1012 user access information. If user access (account) is changed in any of the following ways and is therefore
1013 inconsistent with the contents of the authoritative baseline (i.e., the contents of all the directories), the
1014 Monitoring capability detects this inconsistency and generates an alert:

- 1015 ▪ via direct manipulation of directory information such as an account change, addition, or
1016 deletion/deactivation by an insider or malware
- 1017 ▪ temporary removal of a directory from its network for offline manipulation
- 1018 ▪ administrative change mistake by a privileged user via the PAM system

1019 The Security Monitoring capability can detect this inconsistency because every user access information
1020 update and every provisioning operation generates a log message that is sent to the Security Monitoring
1021 capability. For every valid account update, a consistent set of logs is expected to flow from each
1022 capability to the Security Monitoring capability, and the log messages received from all capabilities are
1023 checked for consistency.

1024 In addition, when user access updates are made to each directory, these changes are also propagated to
1025 the VDS, which also sends logs of these updates to the Monitoring capability. Hence, the Security
1026 Monitoring capability also checks to ensure that for each update that is logged at a directory, a
1027 corresponding update is logged by the VDS. The VDS functionality increases the effectiveness of a
1028 directory monitoring program through synchronization and change reporting. This increase will enable
1029 anomalous directory changes to be reported within seconds to minutes, depending on the VDS
1030 capability configuration.

1031 This established set of log data flowing from reference design capabilities to the Security Monitoring
1032 capability is event-based, meaning that the data flow is initiated by specific activities that, once
1033 detected, generate logs (see NIST SP 1800-9C: *How-To Guides* for a list of events logged). The activity at
1034 the affected reference design capability must be identified and then reported to the Security Monitoring
1035 Capability. If the process that is supposed to detect the activity or generate or transmit the log to the
1036 Security Monitoring capability stops working temporarily and then resumes operation, whatever
1037 updates have occurred in the interim will not have generated any logs. In particular, if a change is made

1038 to a directory while it is not connected to the network, no log event is generated at the time of the
1039 change. If the update was the result of a legitimate provisioning operation, the Monitoring capability
1040 detects an inconsistency in the logs received from various capabilities and it generates a false alarm.
1041 However, if the update was performed by an adversary who intentionally modified a directory while it
1042 was offline, this change to the directory could not generate a log, even though the directory contents
1043 would now be inconsistent with the contents of the Provisioning capability and of the VDS. This type of
1044 activity would be detected, and an alert noting that the directory connection was lost by the VDS would
1045 be sent to the Security Monitoring capability.

1046 Monitoring directory update events is not the same as looking at the actual data in the directories. Log
1047 collection and transmission is typically performed as a best-effort process. Log collection agents
1048 sometimes go down, and they can be fragile, so there would be some risk inherent in relying solely on
1049 reference design capabilities to self-report activities and updates. If a directory update event were to
1050 somehow fail to reach the Security Monitoring capability, there would be no way to know that the
1051 change was made without looking at the information in the directory.

1052 To mitigate the possibility that the best-effort nature of event-based reporting could be exploited to
1053 populate a directory with unauthorized information in this way, the VDS is configured to monitor the
1054 connections that it has with each of the directories, thereby ensuring that these connections are up. If
1055 any of the directories go offline or if its connection with the VDS goes down for any reason, this event
1056 would be signaled to the Security Monitoring capability. In addition, the VDS is configured to cache the
1057 directory information that it has stored. Once the cache has been initialized and caching has been
1058 turned on, the VDS monitors the user access information for any changes. When it detects a change or a
1059 connection being re-established to a directory that had been offline, the VDS compares the access
1060 information it has cached with the values present in the directories. If there are any discrepancies, it
1061 creates a log of these and sends the log to the Security Monitoring capability, enabling the Security
1062 Monitoring capability to detect unauthorized changes to the directories. If the reference design incurs
1063 too much of a performance hit because of the VDS cache information volume, a separate server can be
1064 set up to store the VDS's view of user access information for comparison with the actual contents of the
1065 directories. The reference design should not rely solely on the monitoring and flow of event-based logs
1066 to ensure that no unauthorized changes have been made to the directories; regular auditing of actual
1067 directory contents is also important to reduce risk and bring additional value.

1068 In many cases, an organization's ARM system could have started out simply using a single directory, but,
1069 as a consequence of mergers and acquisitions, other applications, resources, and directories were
1070 added. As a result, an organization might not have complete awareness of the extent of any given user's
1071 access control authorizations across all appliances. Practically, an organization that deploys the
1072 reference design will want to ensure that it converts from the policies that it is enforcing at the time of
1073 adoption to the policies that it seeks to enforce. Simply adopting the reference design does not cause an
1074 organization to automatically begin enforcing its desired access control policy. The objective of
1075 reference design is to ensure the integrity of access changes as updates are applied. How well an

1076 organization enforces the access control policies overall depends on the initial baseline contents of
1077 those directories. Certifying that these initial baseline contents are correct is not addressed in the
1078 design. Planning for deployment of the design gives an organization the opportunity to go back and
1079 audit the access control information in their directories and get a more global, correlated,
1080 disambiguated view of the user access roles and attributes that are currently in effect.

1081 Ideally, in an operational deployment of the reference design, a separate system would also be
1082 deployed to periodically examine the directory contents to verify that they enforce enterprise policies as
1083 intended. Having such a system enables a security analyst to determine when an access control mistake
1084 is the result of a breakdown in business process as opposed to being the result of a security breach or
1085 technology failure.

1086 *6.4.1.14 DE.AE-3: Event data are aggregated and correlated from multiple sources and*
1087 *sensors*

1088 The Security Monitoring capability aggregates and correlates user access information change event logs
1089 from three types of sources:

- 1090 ▪ User Access Information Provisioning capability
- 1091 ▪ each of the directories (which, in aggregate, constitute the authoritative/baseline source)
- 1092 ▪ Virtual Directory capability

1093 If any inconsistencies in the user access data changes across these sources are detected, an alert is
1094 generated. The Security Monitoring capability also receives log information from the PAM and the
1095 Virtual Environment PAM capabilities and generates an alert if it detects privileged user access attempts
1096 that are not consistent with the user access information that it has received from other reference design
1097 capabilities.

1098 *6.4.1.15 DE.AE-5: Incident alert thresholds are established*

1099 The alert thresholds are binary: if the user access information logs that the Security Monitoring
1100 capability receives from each of its sources are not consistent with each other, an alert is generated. If
1101 the user access information logs received from the various capabilities are consistent with each other,
1102 no alert is generated.

1103 *6.4.1.16 DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events*

1104 All activity of privileged users on physical reference design capabilities is monitored and logged by the
1105 PAM capability for OSs and applications. Similarly, all activity that virtual machine (VM) Administrators
1106 perform on VMs (but not the activity that they perform on the OSs installed on those VMs) is logged by
1107 the VE PAM. The administrators of the OSs and applications running on VMs make use of the PAM
1108 capability for access. These capabilities log each administrator's activity on either the physical console or
1109 the VM and send the logs to the Monitoring capability. They also generate alerts when operations that

1110 are not authorized are attempted. The Security Monitoring capability monitors the alerts generated by
1111 these physical and virtual PAM capabilities to detect potential cybersecurity events.

1112 **6.5 Security of the Reference Design**

1113 The list of reference design capabilities in Table 6-1 focuses on the access control capabilities of the
1114 reference design that are needed to enable it to meet its objective of automating the management of
1115 user access information (accounts). Table 6-1 does not focus on capabilities needed to manage and
1116 secure the reference design. However, the reference design itself must be managed and secured. To this
1117 end, this second part of the security evaluation focuses on the security of the reference design.

1118 Measures implemented to protect the reference design from outside attack include:

- 1119 ▪ isolating certain capabilities on separate subnetworks protected by firewalls
- 1120 ▪ implementing a management network to isolate log and management traffic from the
1121 production (business operations) networks
- 1122 ▪ securing critical user access information and logs to protect them from unauthorized insertion,
1123 modification, or deletion
- 1124 ▪ logging of all privileged user access activities
- 1125 ▪ encryption and integrity protection of user access information and logs while this information is
1126 in transit between capabilities

1127 Table 6-2, Capabilities for Managing and Securing the ARM Reference Design, describes the security
1128 protections each capability provides and lists the corresponding products that were used to instantiate
1129 each capability. The security evaluation focuses on the capabilities rather than the products. The NCCoE
1130 is not assessing or certifying the security of the products included in the example implementation. We
1131 assume that the enterprise already deploys network security capabilities such as firewalls and intrusion
1132 detection devices that are configured according to best practices. The focus here is on securing
1133 capabilities introduced by the reference design and minimizing their exposure to threats.

1134 **Table 6-2 Capabilities for Managing and Securing the ARM Reference Design**

1135 This table describes only the product capabilities and CSF subcategory support used in the reference architecture. Many of the products have
 1136 significant additional security capabilities that are not listed here.)

Capability	Specific Product	Function	CSF Subcategories
Subnetting	N/A	Technique of segmenting the network on which the reference design is deployed so that capabilities on one subnetwork are isolated from capabilities on other subnetworks. If an intruder can gain access to one segment of the network, this technique limits his or her ability to monitor traffic on other segments of the network. For example, the enterprise’s production network, on which user access information and decisions are conveyed, is separate from the reference design’s monitoring and management subnetwork.	PR.DS-1: Data-at-rest is protected. PR.PT-4: Communications and control networks are protected.
User Access Information Repository Firewall	PFSense	Sits between one or more directories and the rest of the reference design, with one interface connecting to the subnetwork that is dedicated to the directories and a second interface connecting to the rest of the reference design. Monitors all traffic that flows to and from the directories. This firewall is configured to permit only the required ports and protocols (e.g., LDAPS) to be exchanged between the User Access Information Provisioning capability and the directory and between the VDS capability and the directory. Privileged user access to this firewall (i.e., access of all users authorized to change firewall rules) must be managed through the Privileged Access Management capability.	PR.PT-4: Communications and control networks are protected.

Capability	Specific Product	Function	CSF Subcategories
<p>Privileged Access Management</p>	<p>TDi Technologies ConsoleWorks</p>	<p>Manages privileged access to the OSs of all physical reference design capabilities. This is the single portal into which all users with administrator privileges must log in; it defines what systems these administrators are authorized to access based on their role and attributes. It also logs every keystroke that is performed by users with administrator privileges, creating an audit trail of privileged user access to the OSs of the physical systems that are hosting reference design capabilities. Allowed commands can also be identified to further control administrator actions.</p>	<p>PR.AC-3: Remote access is managed. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.</p>
<p>Virtual Environment Privileged Access Management</p>	<p>HyTrust Cloud Control</p>	<p>Manages privileged access to the virtual environment (including machines, switches, and host hardware) that host reference design capabilities. Cloud Control is the single portal into which all users with administrator privileges to virtual environment systems must log in; it defines what VMs these administrators are authorized to access based on the user's role and attributes. It logs activity that administrators perform on VMs, but it does not log operations that are performed on the OSs that are installed on those VMs. These logs create an audit trail of privileged user access in the virtual environment that is hosting the reference design capabilities.</p>	<p>PR.AC-3: Remote access is managed. PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties. PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.</p>

Capability	Specific Product	Function	CSF Subcategories
Log Integrity	Splunk Forwarder	<p>Forwards log information from each reference design capability to the Monitoring capability. This capability encrypts log files before sending them, thereby providing them with both integrity and confidentiality while in transit.</p> <p>If an alternative product were used to instantiate this capability, it could add a time stamp and hash/integrity seal to each log file instead, thereby providing the file with integrity, but not confidentiality, protections. However, if the hash/integrity seal were to continue to be stored with the log file at the Monitoring capability, it would provide a mechanism to detect unauthorized modifications made to the log file while stored there.</p>	<p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p> <p>PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.</p> <p>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.</p> <p>DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.</p> <p>PR.DS-2: Data-in-transit is protected.</p>

1137

1138 6.5.1 Securing New Attack Surfaces

1139 The reference design introduces new capabilities into the enterprise, and with any new capability comes
1140 the potential for new attack surfaces. Implementation of this reference architecture necessitates
1141 securing potential attack surfaces. To safeguard the internal systems covered under the proposed ARM
1142 system, the following steps can be taken:

- 1143 1. **Points of entry.** The reference design enables employee access to be enabled, modified, and
1144 disabled from a single management system that provisions user access information changes to
1145 all directories within the enterprise. To prevent the reference design's converged provisioning
1146 capability from being transformed into an advantage for the adversary, the organization must
1147 secure logical and physical access to the Policy Management, Policy Administration, and User
1148 Access Information Provisioning capabilities, in addition to controlling access to the individual
1149 directories themselves.
- 1150 2. **Disabling monitoring.** Consistency between the contents of this virtual directory and each of
1151 the individual physical directories is used to determine if any changes were made to the
1152 contents of the directories (and therefore unable to send log messages documenting these
1153 changes to the Security Monitoring capability). To ensure the reference design's Security
1154 Monitoring capability receives the proper log messages from the VDS, prevent unauthorized
1155 access to the VDS.
- 1156 3. **Sabotaging detection.** Aggregation of user access information and logs in the Security
1157 Monitoring capability provides enormous potential in terms of anomaly detection. To prevent
1158 malicious changes to the security logs within the Security Monitoring capability, ensure
1159 unauthorized access to its contents is blocked.

1160 6.5.1.1 Securing Access to the Policy Administration Capability

1161 User access information changes are not typically made from within any user accounts on the Policy
1162 Administration capability, which could be misused to cause the unauthorized modification of user access
1163 information or workflows. Typically, user access information changes are initiated via a bulk update
1164 from a human resource system. User access information updates are input via .csv files that the Policy
1165 Administration capability receives from the HR system. HR administrators who are authorized to do so
1166 create .csv files and feed them into the Policy Administration capability. By policy, workflows, which are
1167 essentially business process rules that can be defined to enforce access (and other) policy, should be
1168 established to ensure that no single HR administrator can perform updates in isolation. Workflows
1169 based on the principles of least privilege and separation of duties should be defined that ensure that
1170 before updates are performed, multiple HR administrators and or multiple administrative approvals
1171 must be received. It should not be possible to submit a fake, unauthorized .csv file to the Provisioning
1172 capability; the Provisioning capability should only accept .csv files from the HR system with appropriate
1173 approvals in the context of a defined workflow.

1174 *6.5.1.2 Securing Access to the Policy Management Capability*

1175 The ability to create and modify user access policies within the Policy Management capability must also
1176 be carefully controlled. By policy, workflows should be established to ensure that no single
1177 administrator can create or modify policies in isolation. Workflows based on the principles of least
1178 privilege and separation of duties should be defined to ensure that before updates are performed,
1179 multiple administrators and or multiple administrative approvals must be received. It should not be
1180 possible to submit policies that have not been properly vetted and approved in the context of a defined
1181 workflow.

1182 *6.5.1.3 Securing Access to the User Access Information Provisioning Capability*

1183 The User Access Information Provisioning capability initiates provisioning activity on the various
1184 directories based on input that is received at the Policy Administration and Policy Management
1185 capabilities and that propagates to the User Access Information Provisioning capability. The provisioning
1186 capability should not accept direct input from any source other than the Policy Administration
1187 capability.

1188 *6.5.1.4 Securing Access to the Security Monitoring and Analytics Capability*

1189 If an adversary could modify the contents of the Monitoring capability without detection, it is essentially
1190 “game over” with respect to the ability of the reference design to monitor all access rights changes. By
1191 policy, only security analysts, whose role is to be notified of alerts and examine the logs pertinent to
1192 those alerts to determine if there is a genuine security event, should be able to view logs, and the logs
1193 should be only accessible via read-only access. Workflows based on the principles of least privilege and
1194 separation of duties should be defined to ensure that before any changes to the monitoring analytics are
1195 performed, multiple administrators and or multiple administrative approvals are received. It should not
1196 be possible to create or modify analytics that have not been properly vetted and approved.

1197 As with other reference design capabilities, both policy and the fact that the Monitoring capability’s
1198 console password is secured across multiple vaults should help ensure that the only way privileged users
1199 can access the Monitoring capability for administration is via the PAM capability. The PAM capability, as
1200 has been stated, logs all privileged activity that is performed on the Monitoring capability. However, it
1201 sends these logs to the Monitoring capability. If an inside adversary can misuse his or her privileges on
1202 the Monitoring capability to compromise that capability, it is likely that he or she can also configure the
1203 Monitoring capability to ignore, delete, or modify the logs that it receives from the PAM documenting
1204 this nefarious activity. To truly protect the Monitoring capability, it would be necessary to ensure that all
1205 PAM logs of activity performed on the Monitoring capability are sent to a separate “monitor of
1206 monitors” capability, rather than to the Monitoring capability. Such protection against privileged access
1207 management abuse is important, but it is not addressed in the reference design.

1208 6.5.2 Ensuring Information Integrity

1209 As mentioned earlier, access to each reference design capability must be secured to prevent
1210 unauthorized modification or deletion of access policies, user access information, and analytics
1211 information that is stored in these capabilities. In addition to preventing access to this information while
1212 it is stored in these capabilities, the information must be protected from modification while it is in
1213 transit between reference design capabilities. If user access or policy information were to be deleted,
1214 modified, or falsified while in transit between capabilities, the result would be a loss of confidence in the
1215 access authorization and authentication of users. It is essential that the user access and policy
1216 information have at least its integrity and ideally its confidentiality protected when in transit between
1217 capabilities. Securing communications among all capabilities is essential to securing the reference
1218 design. To provide this protection, all information sent to and from directories and the VDS is encrypted
1219 using the transport layer security (TLS) protocol.

1220 All logs sent within the reference design are encrypted in transit to ensure the confidentiality and
1221 integrity of the log information while it is in transit from the reference design capability that is the
1222 source of the log to the Monitoring capability. Once the log file is transmitted to the Monitoring
1223 capability, it is stored in the clear (i.e., in plaintext form), where it would be vulnerable to modification
1224 or deletion if an adversary were somehow able to gain unauthorized access to the Monitoring capability.

1225 6.5.3 Privileged Access Management

1226 Ideally, as a basic security principle, the privileged user access information that is consulted to manage
1227 access to the reference design (i.e., to manage privileged access to reference design capabilities and the
1228 information they contain) should not be provisioned, stored, or managed by the reference design itself.
1229 Access information for privileged users should be managed by a system separate from the reference
1230 design, and all privileged access should be monitored and logged for auditing and accountability
1231 purposes. The responsibilities of controlling access to reference design capabilities and monitoring and
1232 logging privileged actions performed on these capabilities fall under the discipline of PAM.

1233 6.5.3.1 Privileged Users

1234 The access rules defined within the reference design should incorporate the principles of least privilege
1235 and separation of duties. Users should be given the authority to access only those resources that they
1236 need to access to fulfill their duties, and nothing more. As a result, unprivileged users can log in to their
1237 desktops and access specific resources on the production network that they need to do their jobs, but
1238 they are not authorized to log in to any of the capabilities in the reference design.

1239 We would expect any organization that adopts the reference design to have several classes of privileged
1240 users who are authorized to access reference design capabilities or the machines on which they are
1241 running for the purposes of administering those capabilities and machines.

1242 *6.5.3.2 Insider Threat*

1243 The reference design securely provisions and stores user access information for unprivileged users,
1244 thereby ensuring that if an adversary gains insider access to the organization as an unprivileged user, the
1245 damage that he will be able to do will be restricted to only those resources to which his role gives him
1246 access and limited by what he is authorized to do with those resources. As an unprivileged employee, he
1247 will not have access to reference design capabilities or to the information stored on them, so the
1248 reference design itself should be secure from an unprivileged insider threat. The extent to which the
1249 reference design is protected against a privileged insider threat, however, depends on the privileged
1250 access management solution with which the reference design is integrated. Although comprehensive
1251 mitigation of the privileged insider threat is important, privileged access management is not addressed
1252 in this document.

1253 *6.5.3.3 Privileged User Access Information Storage*

1254 As mentioned earlier, the reference design includes PAM mechanisms for demonstration purposes, but
1255 these mechanisms are not intended to provide a comprehensive PAM solution. In particular, as one
1256 shortcut, the reference design stores the user access information that is consulted to determine who
1257 has privileged access to the PAM in the reference design itself (i.e., in the AD directory), rather than in a
1258 separate system for privileged user access information. This means that when a user logs in to the PAM
1259 capability, for example, the AD directory is consulted to determine if that user should be granted access
1260 and what privileges he or she should have. So, it is the contents of the AD that determine whether a
1261 user should have access to the PAM capability, but it is the PAM capability that determines whether a
1262 user should have the privilege to modify the content of the AD. As a result of this cyclical dependency,
1263 the Console Administrator for the AD directory could, in theory, log in to the console of the machine
1264 hosting the AD directory and add the necessary account and attribute information required to give
1265 himself PAM privileges that would enable him to access to all reference design machines via the PAM. It
1266 should be noted that the reference solution would detect these particular attacks because the
1267 Monitoring capability would generate an alert when it receives logs indicating that AD directory
1268 modifications occurred, when it does not receive corresponding logs from other reference design
1269 capabilities. In addition, policy and workflow precautions, such as requiring multiple parties to agree to
1270 changes to privileged accounts, could be implemented to try to mitigate the threat of such privilege
1271 escalation attacks. Solving these types of insider threats in general is beyond the scope of the reference
1272 design. However, they demonstrate the importance of integrating the reference design with a
1273 comprehensive PAM solution.

1274 *6.5.4 Isolating Reference Design Capabilities from Each Other*

1275 As mentioned earlier, each of the following sets of reference design capabilities is situated on its own
1276 separate subnetwork to isolate these capabilities from each other:

- 1277 ▪ Policy Administration, Policy Management, User Access Information Provisioning, and Virtual
1278 Directory capabilities
- 1279 ▪ Security Monitoring and Analytics capability and Privileged Access Management capability
- 1280 ▪ Virtual Environment Privileged Access Management capability
- 1281 ▪ Directories

1282 Each of the reference design subnetworks is also isolated, via subnetting, from the enterprise’s
1283 production network (backbone network).

1284 Each subnetwork is separated from the rest of the reference design by a firewall that is configured to
1285 restrict the type of data that flow into and out of the subnetwork to the minimum set of necessary
1286 protocols. The ports and protocols to which each firewall restricts access are documented in NIST SP
1287 1800-9C: *How-To Guides*.

1288 *6.5.4.1 Addressing Attacks*

1289 We used the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) model and
1290 framework developed by The MITRE Corporation to identify the following adversary tactics and
1291 techniques that the reference design protects against:

- 1292 ▪ Privilege escalation results when an adversary obtains a higher level of permissions on a system
1293 or network than he is authorized to have.
 - 1294 • An adversary employing the tactic of privilege escalation might use the technique of trying
1295 to modify his user access information attributes that are stored in the enterprise
1296 directories so that these attributes permit him to have more access authority than he is
1297 entitled.

1298 The reference design protects against privilege escalation through its use of logging and
1299 monitoring, which enables it to detect unauthorized changes in user attribute information.

- 1300 • Alternatively, an adversary attempting to achieve privilege escalation could use the
1301 technique of creating an account for a new (nonexistent) user in one of the enterprise’s
1302 directories and giving that new user the desired higher level of privileges.

1303 If such an account is created in a directory directly rather than being provisioned via the
1304 Policy Administration and Provisioning capabilities, the Security Monitoring capability is
1305 designed to detect that the account was not created using the converged provisioning
1306 system and generate an alert.

- 1307 ▪ Credential access results when an adversary obtains access to enterprise resources that he is not
1308 authorized to access. An adversary employing the tactic of credential access could use the
1309 technique of trying to obtain legitimate user credentials that belong to another user by
1310 eavesdropping on these credentials as they are sent to and from directories in the network.

1311 The reference design protects against credential access through its use of LDAPS (secure socket
1312 layer-based encrypted traffic between LDAP servers and clients), which prevents the network
1313 from sniffing another user's credentials.

1314 6.5.5 Deployment Recommendations

1315 When deploying the reference design in an operational environment, organizations should follow
1316 security best practices to address potential vulnerabilities and ensure that all assumptions on which the
1317 solution relies are valid to minimize any risk to the production network. Organizations leveraging the
1318 reference design should adhere to the following list of recommended best practices that are designed to
1319 reduce risk. Note that the laboratory instantiation of the reference design did not implement every
1320 security recommendation. They should not, however, consider this list to be comprehensive; merely
1321 following this list will not guarantee a secure environment. Planning for deployment of the design gives
1322 an organization the opportunity to go back and audit the access control information in their directories
1323 and get a more global, correlated, disambiguated, view of the user access roles and attributes that are
1324 currently in effect.

1325 6.5.5.1 Patch, Harden, Scan, and Test [5]

- 1326 ▪ Keep OSs up to date by patching, version control, and monitoring indicators of compromise
1327 (e.g., performing virus and malware detection as well as keeping anti-virus signatures up to
1328 date).
- 1329 ▪ Harden all capabilities: all capabilities should be deployed on securely configured OSs that use
1330 long and complex passwords and are configured according to best practices.
- 1331 ▪ Scan OSs for vulnerabilities.
- 1332 ▪ Test individual capabilities to ensure that they provide the expected CSF subcategory support
1333 and that they do not introduce unintended vulnerabilities.
- 1334 ▪ Evaluate reference design implementations before going operational with them.

1335 6.5.5.2 Other Security Best Practices [6]

- 1336 ▪ Install, configure, and use each capability of the reference design according to the capability
1337 vendor's security guidance.
- 1338 ▪ Change the default password when installing software.
- 1339 ▪ Identify and understand which pre-defined administrative and other accounts each capability
1340 comes with by default to eliminate any inadvertent back doors into these capabilities. Disable all
1341 unnecessary pre-defined accounts and, even though they are disabled, change their default
1342 passwords (just in case some future patch to the capability enables these accounts).

- 1343 ▪ Segregate reference design capabilities onto their own subnetwork, separate from the
1344 production network, either physically or by using virtual private networks and port-based
1345 authentication or similar mechanisms.
- 1346 ▪ Protect the various reference design subnetworks from each other and from the production
1347 network using security capabilities such as firewalls and intrusion detection devices that are
1348 configured according to best practices.
- 1349 ▪ Configure firewalls to limit connections between the reference design network and the
1350 production network, except for connections needed to support required internetwork
1351 communications to specific IP address and port combinations in certain directions.
- 1352 ▪ Configure and verify firewall configurations to ensure that data transmission to and from
1353 reference design capabilities is limited to only those interactions that are needed. All
1354 communications that are permitted should be restricted to specific protocols and IP address and
1355 port combinations in specific directions.
- 1356 ▪ Monitor the firewalls that separate the various reference design subnetworks from one another.
- 1357 ▪ NIST SP 1800-9C: *How-To Guides* contain the firewall configurations that show the rules that
1358 were implemented in each of the firewalls for the example implementation. These
1359 configurations are provided to enable the reader to reproduce the traffic filtering/blocking that
1360 was achieved in the implementation.
- 1361 ▪ Apply encryption or integrity-checking mechanisms to all information exchanged between
1362 reference design capabilities (i.e., to all user access, policy, and log information exchanged) so
1363 that tampering can be detected. Use only encryption and integrity mechanisms that conform to
1364 most recent industry best practices. Note that in the case of directory reads and writes,
1365 protected mode is defined as the use of LDAPS (RFC 2830).
- 1366 ▪ Strictly control physical access to both the reference design and the production network.
- 1367 ▪ Deploy a separate, complete system for PAM.
- 1368 ▪ Deploy a configuration management system to serve as a “monitor of monitors” to ensure that
1369 if any changes are made to the list of information logged and reported to the Monitoring
1370 Capability or to the analytics in the Monitoring Capability, notifications will be generated. Such a
1371 system could also serve to monitor whether reference design Monitoring capabilities such as log
1372 integrity capabilities or the Monitoring Capability itself go offline or stop functioning and
1373 generate alerts when these capabilities become unresponsive.
- 1374 ▪ Deploy a system that audits and analyzes directory contents to create a description of who has
1375 access to what resources and validate that these access permissions correctly implement the
1376 enterprise’s intended business process and access policies.

1377 6.5.5.3 *Policy Recommendations*

- 1378 ▪ Define the access policies to enforce the principles of least privilege and separation of duties.

- 1379 ▪ Equip the Monitoring capability with as complete a set of rules as possible to take full advantage
1380 of the ability to identify anomalous situations that can signal a cyber event. Define enterprise-
1381 level workflows that include business and security rules to determine each user's access control
1382 authorizations and ensure that enterprise access control policy is enforced as completely and
1383 accurately as possible.
- 1384 ▪ Develop an attack model to help determine the types of things that should generate alerts.
- 1385 ▪ Grant only a very few users (e.g., human resource administrators) the authority to modify
1386 (initiate, change, or delete) employee access information. Require the approval of more than
1387 one individual to be received to initiate employee access information updates. Log all employee
1388 access information modifications that are made. Define workflows to enforce these
1389 requirements.
- 1390 ▪ Grant only a very few users (e.g., access rules administrators) the authority to modify (initiate,
1391 change, or delete) access rules. Require the approval of more than one individual to be received
1392 to initiate access rule updates. Log all access rule modifications that are made. Define workflows
1393 to enforce these requirements.
- 1394 ▪ Grant only a very few users (e.g., security analyst) the authority to modify (initiate, change, or
1395 delete) the analytics that are applied to log information by the Monitoring capability to
1396 determine what constitutes an anomaly and generates an alert. Any changes made to the
1397 analytics should, by policy, require the approval of more than one individual, and these changes
1398 should themselves be logged, with the logs sent to a monitor-of-monitors system other than the
1399 Monitoring Capability and to all security analysts and other designated individuals. Define
1400 workflows to enforce these requirements.

1401 6.5.5.4 *Privileged Access Recommendations* [7]

- 1402 ▪ Deploy a separate, complete system for privileged access management.
- 1403 ▪ Limit the number of privileged accounts on reference design capabilities to one or two specific
1404 console administrators (if the capability is on a physical machine) or virtual administrators (if the
1405 capability is virtual) and a backup administrator account. Limit the number of persons who serve
1406 as console administrator for more than one capability.
- 1407 ▪ Require all users logging in to any reference design capability to do so via the PAM (to ensure
1408 that all privileged user activity is logged and that these logs will be sent to the Monitoring
1409 capability). Forbid all reference design capabilities from having their consoles accessed directly
1410 in a way that bypasses the PAM.
- 1411 ▪ Ensure that any administrative changes to the PAM (i.e., the creation of any new privileged user
1412 accounts, the modification of privileges in privileged user accounts, or a change to the list of
1413 PAM activity that is logged) require, by policy, the approval of more than two individuals. Also,
1414 ensure that all administrative changes to the PAM are logged and will generate notifications.

- 1415 ▪ Require the PAM and VE PAM consoles to be accessed in person rather than permitting them to
1416 be accessed remotely.
- 1417 ▪ Configure the PAM to have an always-on connection to all devices in the reference design so
1418 that it can monitor each device’s console port. This configuration ensures that all activity
1419 performed over the console port will be logged for monitoring and audit purposes. Configure
1420 the PAM such that if it’s always-on connection to any device is disconnected, an alert is
1421 generated. This configuration ensures that security auditors can be aware of any times during
1422 which the console port of a device might have been accessed without the activity being logged
1423 or monitored.

1424 6.6 Security Evaluation Summary

1425 The security benefits of the reference design include:

- 1426 ▪ converged management of user access information and policy
- 1427 ▪ user access information provisioning that is governed by documented and repeatable business
1428 processes (workflows)
- 1429 ▪ rapid provisioning and de-provisioning using consistent, efficient, and automated processes
- 1430 ▪ centralized log storage to support the ability to apply monitoring and analytics across
1431 capabilities to detect potential security events, as well as to easily track and audit all user access
1432 information and policy changes, provisioning requests, and directory modifications.

1433 These convergence, automation, and monitoring capabilities increase the security of organizations that
1434 adopt the reference design.

1435 Automation of the administration and provisioning of user access information enables efficient, quick,
1436 and consistent enforcement of the principles of least privilege and separation of duties with respect to
1437 the access authority granted to each enterprise user. By performing administration and provisioning
1438 automatically, the reference design eliminates the need for individuals or groups of system
1439 administrators to manually modify, monitor, or audit the content of each of the enterprise’s directories.
1440 Such automation improves security by reducing the possibility of human error being introduced during
1441 these processes. It ensures that when users are added or removed, or their responsibilities and the
1442 things they are authorized to do change, the modifications that need to be made to the user access
1443 information that determines what systems they have access to, when they have access to them, and
1444 what they can do on those systems can be provisioned from a single, converged location that
1445 automatically propagates these changes to all directories throughout the enterprise. These access
1446 information changes can be provisioned accurately and consistently throughout the enterprise
1447 instantaneously, ensuring that each employee’s access permissions are synchronized across all
1448 enterprise directories. These capabilities help to reduce the so-called privilege creep that sometimes
1449 occurs as a user’s role changes, and he or she is given access to additional systems without necessarily
1450 having his or her previous access privileges reduced or modified accordingly. Privilege creep can create

1451 opportunities for insider threat attacks. These capabilities also help to reduce the possibility that a
1452 user's access permissions become inconsistent across directories.

1453 The reference design also automatically monitors changes to the content of each directory and supports
1454 an audit system by sending logs from all reference design capability to a single location (the Monitoring
1455 capability). Consolidation of logs from all reference design capabilities at the Monitoring capability
1456 enables the reference design to correlate the logs of updates made to each enterprise directory with
1457 logs from the policy administration and provisioning capabilities and from the VDS in a way that is not
1458 possible when the logs generated by these capabilities are not consolidated at a single location. This
1459 consolidation enables the reference design to ensure that access information updates that are made to
1460 the enterprise's directories are in fact the result of personnel status information modifications input by
1461 HR, defined and approved according to business workflow rules and access policy, and provisioned via
1462 the reference design.

1463 Use of the Monitoring capability has the potential to help eliminate access policy inconsistencies that
1464 could result from human error, as well as to detect security incidents that may be the result of a
1465 deliberate attack. Log consolidation, combined with the ability to monitor and apply analytics to the logs
1466 generated by all reference design capabilities, makes it possible for the reference design to
1467 automatically detect anomalous situations that can indicate a security breach that would be more
1468 difficult, if not impossible, to detect at any single user access information directory being considered in
1469 isolation. In addition, although it does not include an audit solution, the reference design enables
1470 access-related audits to be performed easily and efficiently by aggregating all log information in the
1471 Monitoring capability.

1472 As with any solution, the reference design introduces new capabilities to the enterprise, and with any
1473 new capabilities come new threat surfaces. However, these threats can be mitigated using mechanisms
1474 designed to secure access to the new capabilities and to the user access information and logs that they
1475 exchange and store. In addition, the reference design's security monitoring and analytics capability also
1476 helps mitigate threats by systematically subjecting the logs from all reference design capabilities to
1477 anomaly detection analytics that ensure the authenticity of all directory entries and updates.

1478 **7 Functional Evaluation**

1479 We conducted a functional evaluation of the ARM example implementation, as implemented in our
1480 laboratory, to verify that it worked as expected. The evaluation verified that the example
1481 implementation could perform the following functions:

- 1482 ▪ Assign and provision access information to directories based on a set of organizational access
1483 policy rules.
- 1484 ▪ Create, modify, and deactivate/delete users in directories.
- 1485 ▪ Detect changes to user access information within directories.
- 1486 ▪ Generate a security alert when it detected anomalous activity—specifically, when it detected
1487 changes to any directory without also receiving logs corresponding to these changes from all
1488 other expected ARM capabilities.

1489 Section 7.1 describes the format and components of the functional test cases. Each functional test case
1490 is designed to assess the capability of the example implementation to perform the functions listed
1491 above and detailed in the ARM use case requirements in [Section 7.2](#). SharePoint is used for
1492 demonstration and testing purposes to simulate application and data resources for which access is
1493 managed. Access is controlled via attributes and group membership information stored in the
1494 directories.

1495 **7.1 ARM Functional Test Plan**

1496 This test plan includes the test cases necessary to conduct the functional evaluation of the ARM example
1497 implementation. The ARM example implementation is currently deployed in a lab at the NCCoE. The
1498 implementation tested is described in [Section 5](#).

1499 Each test case consists of multiple fields that collectively identify the goal of the test, the specifics
1500 required to implement the test, and how to assess the results of the test. Table 7-1 provides a template
1501 of a test case, including a description of each field in the test case

1502 Table 7-1 Test Case Fields

Test Case Field	Description
Parent requirement	Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement.
Testable requirement	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.
Associated Security Controls	The NIST SP 800-53 Rev. 4 controls addressed by the test case.
Description	Describes the objective of the test case.
Associated test cases	In some instances, a test case may be based on the outcome of another test case(s). For example, analysis-based test cases produce a result that is verifiable through various means (e.g., log entries, reports, and alerts).
Preconditions	The starting state of the test case. Preconditions indicate various starting state items, such as a specific capability configuration required or specific protocol and content.
Procedure	The step-by-step actions required to implement the test case. A procedure may consist of a single sequence of steps or multiple sequences of steps (with delineation) to indicate variations in the test procedure.
Expected results	The expected results for each variation in the test procedure.
Actual results	The observed results.
Overall result	The overall result of the test as pass/fail. In some test case instances, the determination of the overall result may be more involved, such as determining pass/fail based on a percentage of errors identified.

1503

7.2 ARM Use Case Requirements

1504 Table 7.2 identifies the ARM functional evaluation requirements that are addressed in this test plan and
1505 their associated test cases. The teller application access attribute is held in the OpenLDAP directory and
1506 the loan application access attribute is held in Active Directory. These applications will be referenced
1507 throughout the test plans to verify directory modifications. The NCCoE does not have a mainframe
1508 application that can be used for testing. Therefore, verification of RACF changes will be done manually
1509 through inspection of the directory contents.

1510 Table 7-2 ARM Functional Requirements

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR 1	The ARM example implementation shall include an ARM workflow capability that can create users with policy-driven attributes and group memberships in the following directories:			
CR 1.a		Active Directory		ARM-1
CR 1.b		OpenLDAP		ARM-1
CR 1.c		RACF (via Vanguard)		ARM-1
CR 2	The ARM example implementation shall include an ARM workflow capability that can deactivate users in the following directories:			
CR 2.a		Active Directory		ARM-2
CR 2.b		OpenLDAP		ARM-2
CR 2.c		RACF (via Vanguard)		ARM-2
CR 3	The ARM example implementation shall include a workflow capability that can change an existing user's attributes and group memberships in the following directories:			
CR 3.a		Active Directory		ARM-3
CR 3.b		OpenLDAP		ARM-3
CR 3.c		RACF (via Vanguard)		ARM-3

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR 4	The ARM example implementation shall include a security Monitoring capability that can detect changes to user attributes and group memberships in the following:			
CR 4.a		Active Directory (AD) via logs from:		
CR-4.a.1			AD	ARM-4
CR-4.a.2			Radiant Logic	ARM-4
CR-4.a.3			AlertEnterprise	ARM-4
CR 4.b		OpenLDAP via logs from:		
CR-4.b.1			OpenLDAP	ARM-4
CR-4.b.2			Radiant Logic	ARM-4
CR-4.b.3			AlertEnterprise	ARM-4
CR 4.c		RACF via logs from:		
CR-4.c.1			Vanguard	ARM-4
CR-4.c.2			Radiant Logic	ARM-4
CR-4.c.3			AlertEnterprise	ARM-4
CR 5	The ARM example implementation shall include a security Monitoring capability that will generate			

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
	an alert based on pre-defined anomalous (logged) activity for the following use cases:			
CR 5.a		Active Directory user changes with no correlated log received from:		ARM-5
CR-5.a.1			AD	ARM-5
CR-5.a.2			Radiant Logic	ARM-5
CR-5.a.3			AlertEnterprise	ARM-5
CR 5.b		OpenLDAP user changes with no correlated log received from:		
CR-5.b.1			OpenLDAP	ARM-5
CR-5.b.2			Radiant Logic	ARM-5
CR-5.b.3			AlertEnterprise	ARM-5
CR 5.c		RACF (Vanguard) user changes with no correlated log received from:		
CR-5.c.1			RACF (Vanguard)	ARM-5

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
CR-5.c.2			Radiant Logic	ARM-5
CR-5.c.3			AlertEnterprise	ARM-5

1511

1512 **7.3 Test Case: ARM-1**1513 **Table 7-3 Test Case ID: ARM-1**

Parent requirement	(CR 1) The ARM example implementation shall include an ARM workflow capability that can create users with policy-driven attributes and group memberships in the following directories.
Testable requirement	(CR 1.a) Active Directory, (CR 1.b) OpenLDAP, (CR 1.c) RACF
Description	Show that the ARM example implementation can create users in the various directories with the appropriate access and permissions.
Associated test cases	N/A
Associated CSF Subcategories	PR.AC-1, PR.AC-4
Preconditions	<p>HR representative .csv file is available.</p> <p>ARM example implementation is implemented and operational in the lab environment.</p> <p>Standard and privileged user sets are known to the testers.</p> <p>Privileged users are provisioned directly within the ConsoleWorks and HyTrust applications.</p> <p>A set of directories: AD, OpenLDAP and RACF (Vanguard) are operational.</p>
Procedure	<p>Activate ARM workflow engine and run command to read the HR .csv file.</p> <p>Verify that the AlertEnterprise system successfully processes the data.</p> <p>Query the directories to determine if the users are provisioned to the directories with the correct group memberships and attributes as specified by the .csv file.</p> <p>Query the Vanguard RACF system to verify that users are correctly provisioned as expected from the information included in the HR .csv file.</p> <p>At a workstation on the user network, attempt to log in to the teller application as a user known to have access to the teller application. The teller application control attribute is contained in the OpenLDAP directory.</p> <p>At a workstation on the user network, attempt to log in to the loan application as a user known to have access to the loan application. The loan application control attribute is contained in the AD directory.</p>

	<p>At a workstation on the user network, attempt to log in to the teller application as a user known to not have access to the teller application.</p> <p>At a workstation on the user network, attempt to log in to the loan application as a user known to not have access to the loan application.</p>
Expected Results (pass)	<p>Access Allowed (CR 1.a-c) Users with allowed access can log in to loan and teller demo applications.</p> <p>Access Denied (CR 1.a-c) Users without allowed access are unable to log in to loan and teller demo applications.</p>
Actual Results	<p>(example text) This system functioned appropriately and provided the expected results. Users that are known to not have access were unable to log in to the applications. Users that are known to have access to each application were allowed access.</p>
Overall Result	<p>Pass/Fail (with comments)</p>

1514

1515 **7.4 Test Case ARM-2**1516 **Table 7-4 Test Case ID: ARM-2**

Parent requirement	(CR 2) The ARM example implementation shall include an ARM workflow capability that can deactivate users in the following directories:
Testable requirement	(CR 2.a) Active Directory, (CR 2.b) OpenLDAP, (CR 2.c) RACF
Description	Show that the ARM solution can deactivate users in the appropriate directories.
Associated test cases	n/a
Associated CSF Subcategories	PR.AC-1, PR.AC-4
Preconditions	Successful completion of Test Case ARM-1. Create a new HR dataset that deactivates several users in each directory.
Procedure	Perform Test Case ARM-1 to ensure that user accounts have been created in the directories Read the new HR dataset (described in the pre-conditions) by AlertEnterprise. Verify that the AlertEnterprise system successfully processes the data. Query the directories to determine if the user changes are correctly provisioned to the directories. (deactivated) At a workstation on the user network, attempt to log in to the teller application as a user known to previously have had access to the teller application. (successful attempt in ARM-1). At a workstation on the user network, attempt to log in to the loan application as a user known to previously have had access to the loan application. (successful attempt in ARM-1). Query the Vanguard RACF system to verify the users are correctly deactivated as expected from the information included in the HR .csv file.
Expected Results (pass)	User accounts within the directories are deactivated preventing users from gaining access to resources. (CR 2.a-c)
Actual Results	(CR-2) The ARM example implementation shall include an ARM workflow capability that can deactivate users in the following directories: (CR 2.a) Active Directory: Users that previously had an active account are now in a deactivated account status.

(CR 2.b) OpenLDAP: Users that previously had an active account are now in a deactivated account status.

(CR 2.c) RACF: Users that previously had an active account are now in a deactivated account status.

Overall Result

Pass/Fail (with comments)

1517

1518 **7.5 Test Case ARM-3**1519 **Table 7-5 Test Case ID: ARM-3**

Parent requirement	(CR 3) The ARM example implementation shall include a workflow capability that can change an existing user’s attributes and group memberships within the following directories.
Testable requirement	(CR 3.a) Active Directory, (CR 3.b) OpenLDAP, (CR 3.c) RACF
Description	Show that the ARM solution can change user attributes and group memberships within directories.
Associated test cases	CR 1
Associated CSF Subcategories	PR.AC-1, PR.AC-4
Preconditions	Reuse ARM example implementation in the state after ARM-1 is completed. Create a new HR dataset that makes changes to the access permissions to the users in the original dataset. Change allowed to denied and denied to allow for all the users in the dataset.
Procedure	Operate the example implementation to read the new HR file. Choose a set of users with known access and a set of users without access for each of the loan, teller systems, and Vanguard RACF attribute. Use the ARM workflow to deny access for the set of users with known access chosen in 1 above. Use the ARM workflow to allow access for the set of users known to not have access chosen in 1 above. Process the HR dataset with the AlertEnterprise system. Verify that the AlertEnterprise successfully processes the dataset. At a workstation on the user network, attempt to log in to the teller application as a user known (from ARM-1) to have access to the teller application. At a workstation on the user network, attempt to log in to the loan application as a user known (from ARM-1) to have access to the loan application. At a workstation on the user network, attempt to log in to the teller application as a user known (from ARM-1) to not have access to the teller application. At a workstation on the user network, attempt to log in to the loan application as a user known (from ARM-1) to not have access to the loan application.

	<p>Query the Vanguard RACF system to verify the user accesses are correctly changed as expected from the information included in the HR .csv file.</p>
<p>Expected Results (pass)</p>	<p>(CR 3) The ARM example implementation shall include an ARM workflow capability that can change user attributes and group memberships in the following directories: (CR 3.a) Active Directory: Users that had previously had access to the loan application (from ARM-1) no longer have access. Users that had previous not had access to the teller application (from ARM-1) now do have access. (CR 3.b) OpenLDAP: Users that had previously had access to the teller application (from ARM-1) no longer have access. Users that had previous not had access to the loan application (from ARM-1) now do have access. (CR 3.c) RACF: User accesses are changed as expected.</p>
<p>Actual Results</p>	<p>This system functioned appropriately and provided the expected results. (CR 3) The ARM example implementation can change user attributes and group memberships in the following directories: (CR 3.a) Active Directory: Users that had previously had access to the loan application (from ARM-1) no longer have access. Users that had previous not had access to the teller application (from ARM-1) now do have access. (CR 3.b) OpenLDAP: Users that had previously had access to the teller application (from ARM-1) no longer have access. Users that had previous not had access to the loan application (from ARM-1) now have access. (CR 3.c) RACF: User accesses changed as expected.</p>
<p>Overall Result</p>	<p>Pass/Fail (with comments)</p>

1520

1521 **7.6 Test Case ARM-4**1522 **Table 7-6 Test Case ID: ARM-4**

Parent requirement	(CR 4) The ARM example implementation shall include a security monitoring capability that can detect changes to user attributes and group memberships in the following:
Testable requirement	(CR 4.a) Active Directory (CR-4.a.1) AD, (CR-4.a.2) Radiant Logic, (CR-4.a.3) AlertEnterprise (CR 4.b) OpenLDAP (CR-4.b.1) AD, (CR-4.b.2) Radiant Logic, (CR-4.b.3) AlertEnterprise (CR 4.c) RACF (CR-4.c.1) AD, (CR-4.c.2) Radiant Logic, (CR-4.c.3) AlertEnterprise
Description	Show that the ARM solution can detect when user changes occur within the directories.
Associated test cases	CR 1
Associated CSF Subcategories	DE.AE-1, DE.AE-3, DE.AE-5
Preconditions	Reuse ARM example implementation in the state after ARM-1 is completed.
Procedure	<p>Process the HR dataset from Test Case 3 (the one that changes user access information in each of the directories).</p> <p>Check the security monitoring system to verify that the changes made are reported via logs from each of these systems for a change that occurs to a user in AD: AD, Radiant Logic, and AlertEnterprise.</p> <p>Check the security monitoring system to verify that the changes made are reported via logs from each of these systems for a change that occurs to a user in OpenLDAP: OpenLDAP, Radiant Logic, and AlertEnterprise.</p> <p>Check the security monitoring system to verify that the changes made are reported via logs from each of these systems for a change that occurs to a user in RACF (Vanguard): RACF (Vanguard), Radiant Logic, and AlertEnterprise.</p>
Expected Results (pass)	(CR 4) The ARM security monitoring system receives and stores the logs indicating changes to the following directories: (CR 4.a) Active Directory from (CR-4.a.1) AD, (CR-4.a.2) Radiant Logic, (CR-4.a.3) AlertEnterprise (CR 4.b) OpenLDAP from (CR-4.b.1) OpenLDAP, (CR-4.b.2) Radiant Logic, (CR-4.b.3) AlertEnterprise

	(CR 4.c) RACF (Vanguard) from (CR-4.c.1) Vanguard, (CR-4.c.2) Radiant Logic, (CR-4.c.3) AlertEnterprise
Actual Results	<p>This system functioned appropriately and provided the expected results.</p> <p>(CR 4) The ARM security monitoring system receives and stores the logs indicating changes to the following directories:</p> <p>(CR 4.a) Active Directory from (CR-4.a.1) AD, (CR-4.a.2) Radiant Logic, (CR-4.a.3) AlertEnterprise</p> <p>(CR 4.b) OpenLDAP from (CR-4.b.1) OpenLDAP, (CR-4.b.2) Radiant Logic, (CR-4.b.3) AlertEnterprise</p> <p>(CR 4.c) RACF (Vanguard) from (CR-4.c.1) Vanguard, (CR-4.c.2) Radiant Logic, (CR-4.c.3) AlertEnterprise</p>
Overall Result	Pass/Fail (with comments)

1523

1524 **7.7 Test Case ARM-5**1525 **Table 7-7 Test Case ID: ARM-5**

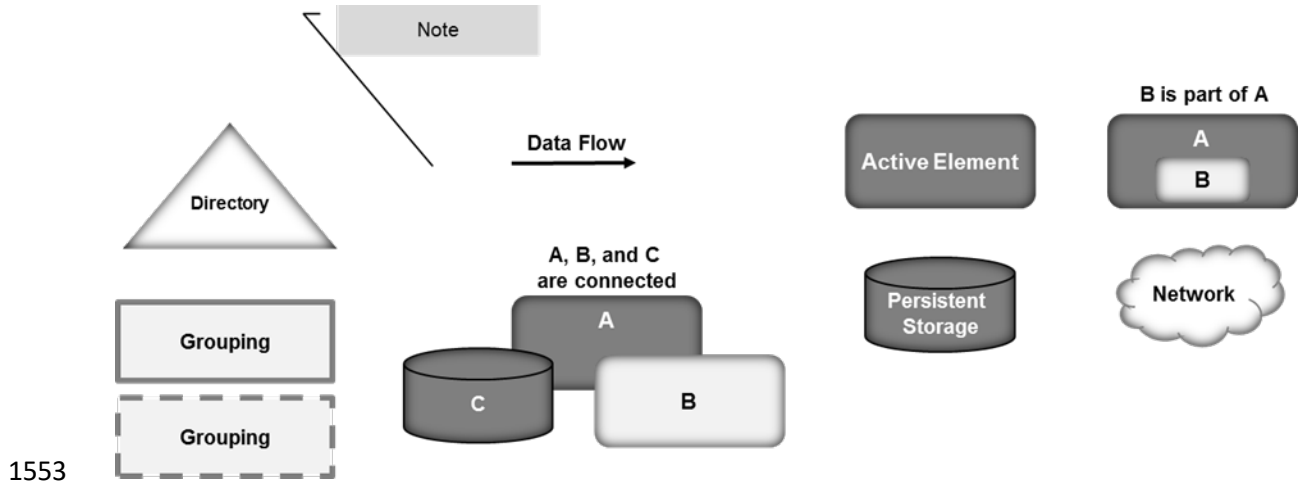
Parent requirement	(CR 5) The ARM example implementation shall include a security monitoring capability that will generate an alert based on pre-defined anomalous (logged) activity for the following use cases:
Testable requirement	<p>(CR 5.a) Active Directory user changes with no correlated log received from: (CR-5.a.1) AD, (CR-5.a.2) Radiant Logic, (CR-5.a.3) AlertEnterprise</p> <p>(CR 5.b) OpenLDAP user changes with no correlated log received from: (CR-5.b.1) OpenLDAP, (CR-5.b.2) Radiant Logic, (CR-5.b.3) AlertEnterprise</p> <p>(CR 5.c) RACF (Vanguard) user changes with no correlated log received from: (CR-5.c.1) RACF (Vanguard), (CR-5.c.2) Radiant Logic, (CR-5.c.3) AlertEnterprise</p>
Description	Show that the ARM example implementation can detect when anomalous user changes occur within the directories.
Associated test cases	CR 1
Associated CSF Subcategories	DE.AE-3, DE.AE-5
Preconditions	Reuse ARM example implementation in the state after ARM-1 is completed.
Procedure	Make a change to each of the directories without the AlertEnterprise provisioning system (anomalous activity) or the privileged account management system. This requires a privileged account on each directory system.
Expected Results (pass)	<p>(CR 5) The ARM example implementation shall include a security monitoring capability that will generate an alert based on pre-defined anomalous (logged) activity for the following use cases: Alert generated for each of the following instances:</p> <p>(CR 5.a) Active Directory user changes with no correlated log received from: (CR-5.a.1) AD, (CR-5.a.2) Radiant Logic, (CR-5.a.3) AlertEnterprise</p> <p>(CR 5.b) OpenLDAP user changes with no correlated log received from: (CR-5.b.1) OpenLDAP, (CR-5.b.2) Radiant Logic, (CR-5.b.3) AlertEnterprise</p> <p>(CR 5.c) RACF (Vanguard) user changes with no correlated log received from: (CR-5.c.1) Vanguard, (CR-5.c.2) Radiant Logic, (CR-5.c.3) AlertEnterprise</p>

<p>Actual Results</p>	<p>This system functioned appropriately and provided the expected results.</p> <p>(CR 5) The ARM example implementation generates an alert based on pre-defined anomalous (logged) activity for the following use cases:</p> <p>Alert were generated for each of the following instances:</p> <p>(CR 5.a) Active Directory user changes with no correlated log received from: (CR-5.a.1) AD, (CR-5.a.2) Radiant Logic, (CR-5.a.3) AlertEnterprise</p> <p>(CR 5.b) OpenLDAP user changes with no correlated log received from: (CR-5.b.1) OpenLDAP, (CR-5.b.2) Radiant Logic, (CR-5.b.3) AlertEnterprise</p> <p>(CR 5.c) RACF (Vanguard) user changes with no correlated log received from: (CR-5.c.1) Vanguard, (CR-5.c.2) Radiant Logic, (CR-5.c.3) AlertEnterprise</p>
<p>Overall Result</p>	<p>Pass/Fail (with comments)</p>

1526 **Appendix A** List of Acronyms

1527	AD	Active Directory
1528	ARM	Access Rights Management
1529	CAT	Cybersecurity Assessment Tool
1530	CR	Capability Requirement
1531	CSF	Cybersecurity Framework
1532	.csv	Comma-Separated Value
1533	DNS	Domain Name Service
1534	FFIEC	Federal Financial Institutions Examination Council
1535	FS-ISAC	Financial Sector Information Sharing and Analysis Center
1536	HR	Human Resources
1537	ID	Identity
1538	IP	Internet Protocol
1539	LDAPS	Lightweight Directory Access Protocol Secure
1540	NCCoE	National Cybersecurity Center of Excellence
1541	NIST	National Institute of Standards and Technology
1542	OS	Operating System
1543	PAM	Privileged Account Management
1544	RACF	Resource Access Control Facility
1545	RMF	Risk Management Framework
1546	SIM	Security Information Management
1547	TLS	Transport Layer Security
1548	VE	Virtual Environment
1549	VDS	Virtual Directory System
1550	VLAN	Virtual Local Area Network
1551	VM	Virtual Machine

1552 **Appendix B Legend for Diagrams**



1554 **Appendix C** **References**

1555

- [1] J. Saltzer, "Protection and the Control of Information Sharing in Multics," *Communications of the ACM*, 17 (7), 388-402 (1974).
- [2] "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology Special Publication 800-53, Rev. 4, April 2013, <http://dx.doi.org/10.6028/NIST.SP.800-53r4>
- [3] "Digital Identity Guidelines," National Institute of Standards and Technology Special Publication 800-63-3, June 2017, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf>.
- [4] "Assessment of Access Control Systems," National Institute of Standards and Technology, NIST Interagency Report 7316, September 2006, <http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf>
- [5] "Guide to Enterprise Patch Management Technologies," NIST Special Publication 800-40 Revision 3, July 2013, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf>
- [6] "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology Special Publication 800-53, Rev. 4, April 2013, <http://dx.doi.org/10.6028/NIST.SP.800-53r4>.
- [7] A Report on the Privilege (Access) Management Workshop, National Institute of Standards and Technology Interagency Report 7657, March 2010, <http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7657.pdf>

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>

DRAFT

DISCLAIMER

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

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

FEEDBACK

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

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

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

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

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

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

64

65 **Contents**

66 **1 Introduction 1**

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 **2 Product Installation Guides 7**

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: AdDOnlineStatus.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 **Appendix A List of Acronyms 297**

187

188 **List of Tables**

189 **Table 1-1 NCCoE Lab Network and System IP Addresses 6**

190 **List of Figures**

191 **Figure 1-1 Logical Access Rights Management Lab Build Architecture 4**

192 **Figure 1-2 Logical Security Log Collection and Monitoring Lab Build Architecture..... 4**

193 **Figure 1-3 NCCoE Lab Networking Diagram 5**

194 **Figure 1-4 NCCoE Lab Networking Diagram 6**

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.

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.

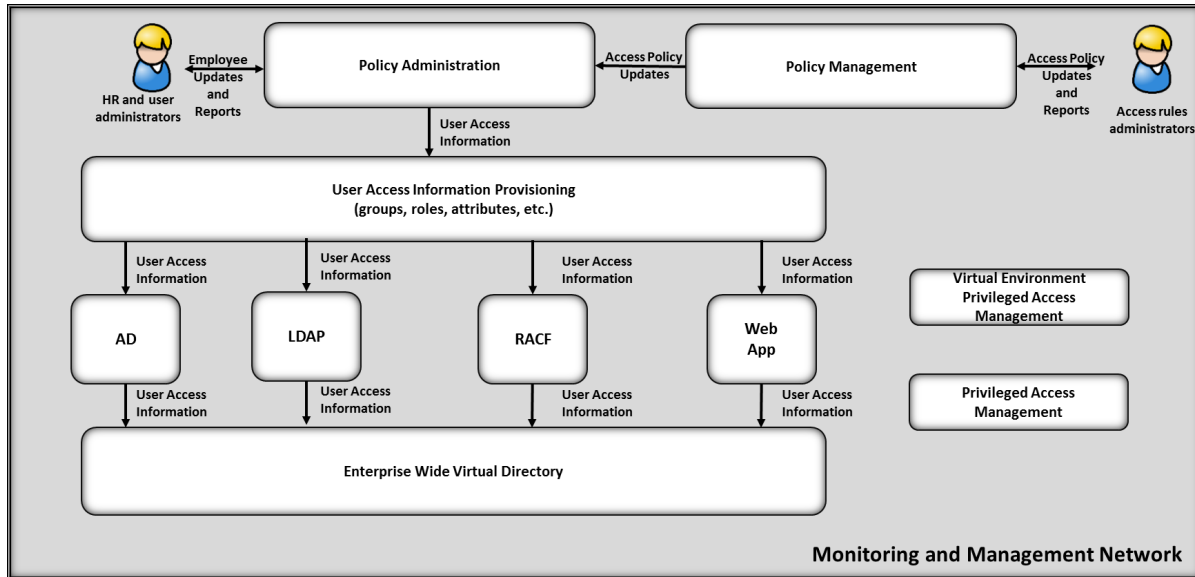
Typeface/ Symbol	Meaning	Example
<i>Italics</i>	filenames and pathnames	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .

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

261 1.4 Logical Architecture Summary

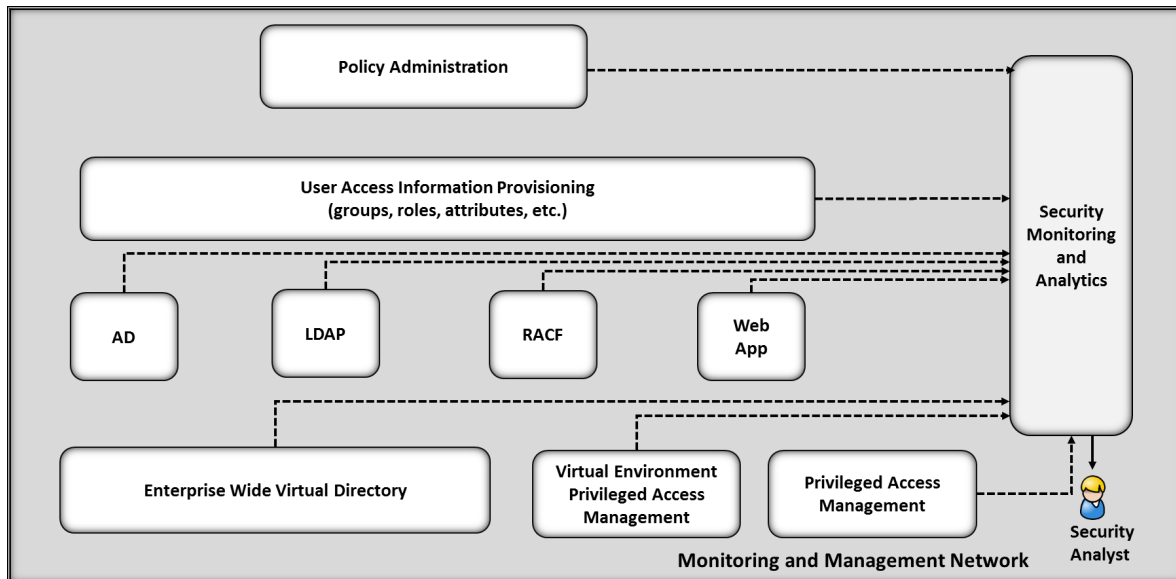
262 NIST Special Publication 1800-9b (SP1800-9b) describes an example implementation consisting of user
 263 access management (including provisioning) and security monitoring / data collection. SP1800-9b
 264 includes a much more detailed description of the architecture for building an instance of the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

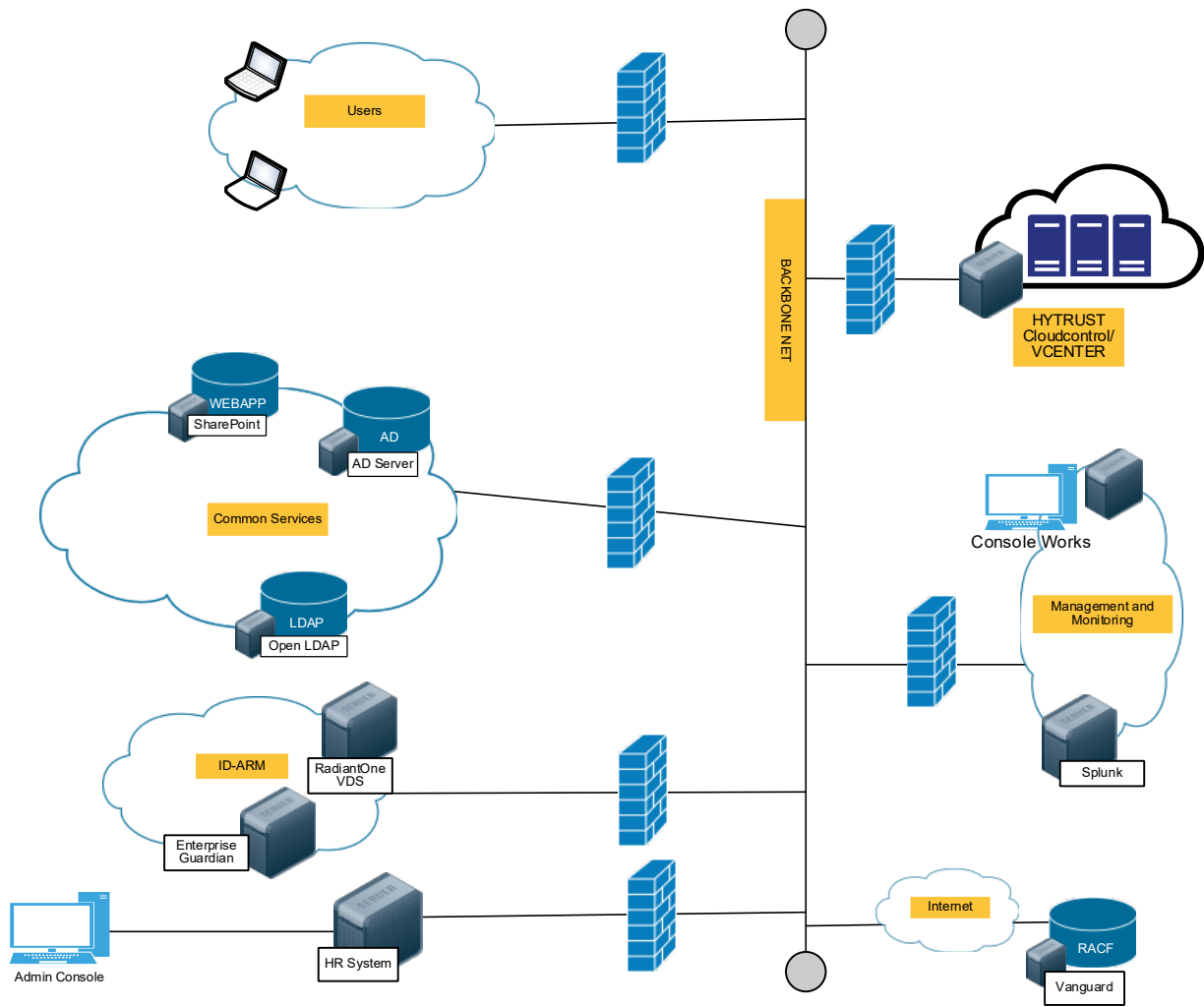
273 **1.5 Network Diagrams**

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**

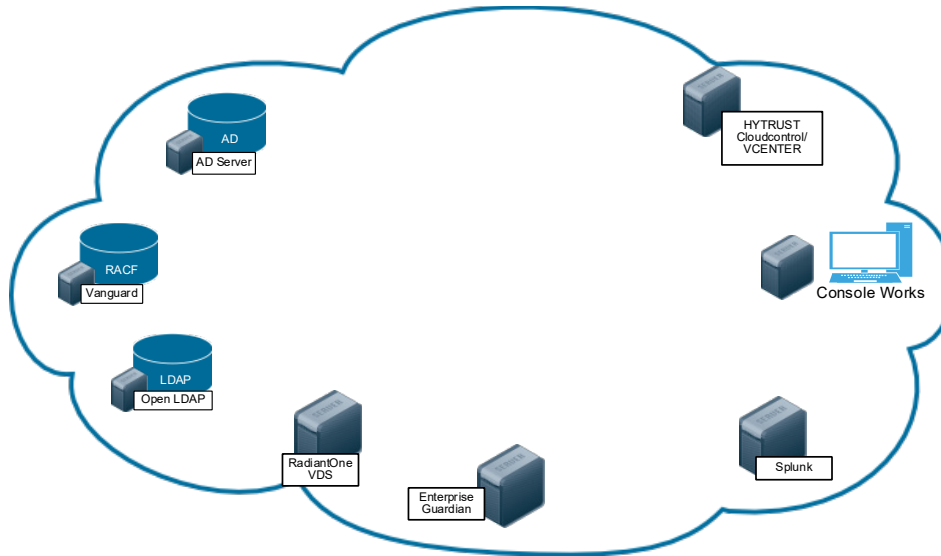
278 Figures 1-3 and Figure 1-4 show the network configurations used in the example implementation.

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

286 **2 Product Installation Guides**

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

290 **2.1 AlertEnterprise**

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

294 **2.1.1 How It's Used**

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

299 **2.1.2 Virtual Machine Configuration**

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

- 301 ▪ Windows Server 2012 R2
- 302 ▪ 1 CPU
- 303 ▪ 2 NICs
- 304 ▪ 32GB Mem
- 305 ▪ 190GB Storage

306 **Network Configuration (Interface 1)**

307 IPv4 Manual
308 IPv6 Disabled
309 IP Address: 192.168.14.113
310 Netmask: 255.255.255.0
311 Gateway: 192.168.14.1
312 DNS Name Servers: 192.168.19.10
313 DNS-Search Domains: acmefinancial.com

314 **Network Configuration (Interface 2)**

315 IPv4 Manual
316 IPv6 Disabled
317 IP Address: 192.168.17.114
318 Netmask: 255.255.255.0
319 Gateway: 192.168.17.1
320 DNS Name Servers 192.168.19.10
321 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%

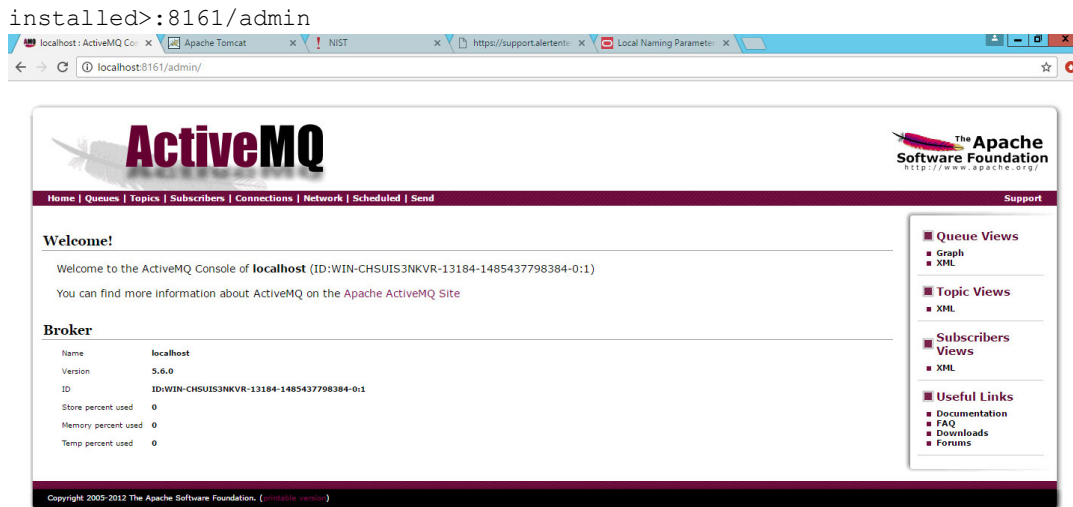
- 344 5. Checking JAVA_HOME and PATH:

```
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



353

354 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
- 357 per the Oracle documentation.

```
File Edit Format View Help
# 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))

ORACL1_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`
- 360 `sys/<password>@pborcl as sysdba.`

361 2.1.7 7-Zip

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

363 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

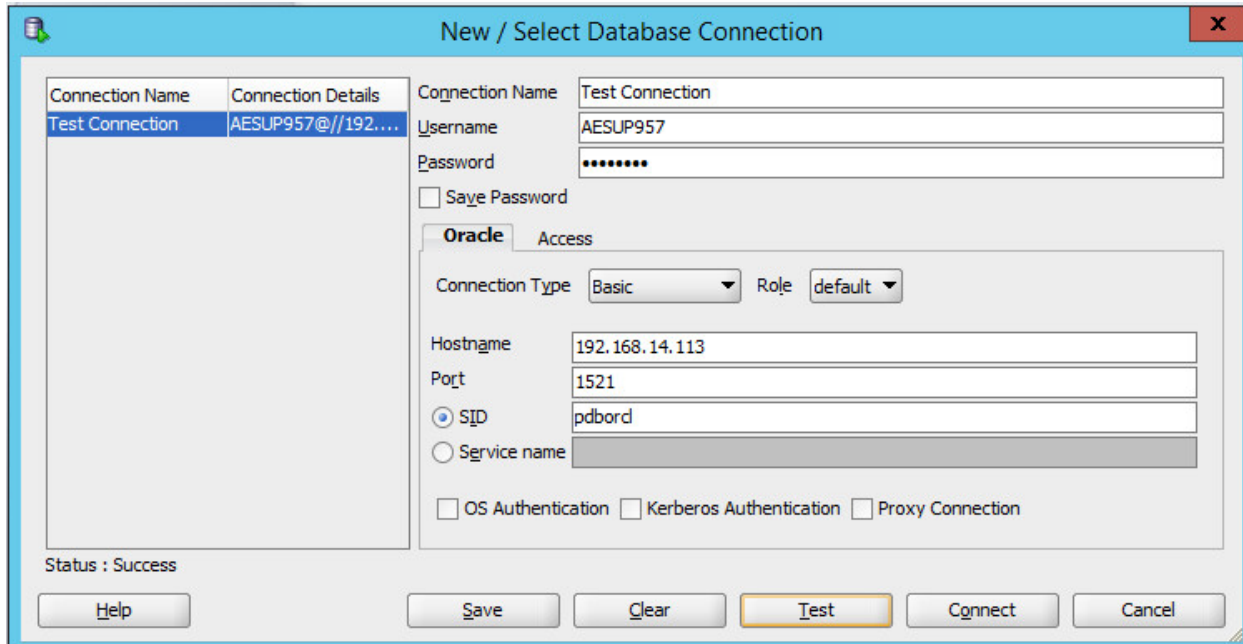
- 370 1. Install the Apache Tomcat Server per the documentation found on the Apache [website](#). Details
 371 can also be found within the *AlertEnterprise Enterprise Guardian Install Guide*.
- 372 a. During the installation, specify the destination folder as **C:\AlertEnterprise\Tomcat**.
- 373 2. When installation is complete, navigate to **Start>Programs>Configure Tomcat** and select the
 374 **Java** tab.
- 375 3. Add the following lines to the end of Java Options, ensuring there are no spaces:
 376 `-XX:PermSize=1024`
 377 `-Xms2048m`
 378 `-Xmx2048m`
 379 `-Dcom.alnt.fabric.loadInitData=force`
 380 `"` `--Dalert.db.update=update`
- 381 4. Click **Apply** and **OK** to close the dialog box.

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

396 2.1.11 Deploying the Application

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

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 `AlertEnterpriseHelp.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.

421 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 unreturnedConnectionTimeout="900" />
```

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

438 2.1.12 Start the Server

- 439 1. Make sure that Active MQ is up and running and then start the Tomcat server.
- 440 2. Start the AlertEnterprise application using the address of the form `http://<Server IP`
 441 `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`.

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

446 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.

452 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,
478 Allow Modify Role
- 479 c. Category – production
- 480 d. Time Zone – Eastern Standard Time
- 481 8. Click **Next**.
- 482 9. Click **Save**.
- 483 10. Repeat Steps 1–9 to add the OpenLDAP and RACF connectors with the following parameters:
- 484 OpenLDAP:
- 485 a. System Type – OpenLDAP Server
- 486 b. Connector Name – OPENLDAP
- 487 c. Connector Description – OpenLDAP
- 488 d. Connector Type – OpenLDAP
- 489 e. HostName – 192.168.19.11
- 490 f. Port Number – 636 (use 389 if SSL is not configured yet)
- 491 g. Service user Dn – CN=Admin,DC=Acmefinancial,DC=com
- 492 h. Password – Fsarm@nccoe1
- 493 i. Use SSL – true (use false if SSL is not configured yet)
- 494 j. User Base DN – OU=Operations,DC=Acmefinancial,DC=com
- 495 k. Group Base DN – OU=Operations,DC=Acmefinancial,DC=com
- 496 l. Object Class – inetOrgPerson
- 497 m. Group Object Class Name – groupOfUniqueNames
- 498 n. Primay Connection – Yes
- 499 o. LastModified Column role – whenChanged
- 500 p. Last Modified User Column – whenChanged
- 501 q. Member Attribute Name for Group – uniqueMember
- 502 r. LDAP DnName – cn
- 503 s. LDAP Account Control Column Name – cn
- 504 t. User Password attributed – default
- 505 u. Encode Password Required? – default
- 506 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

564 2.1.15 User Data Source

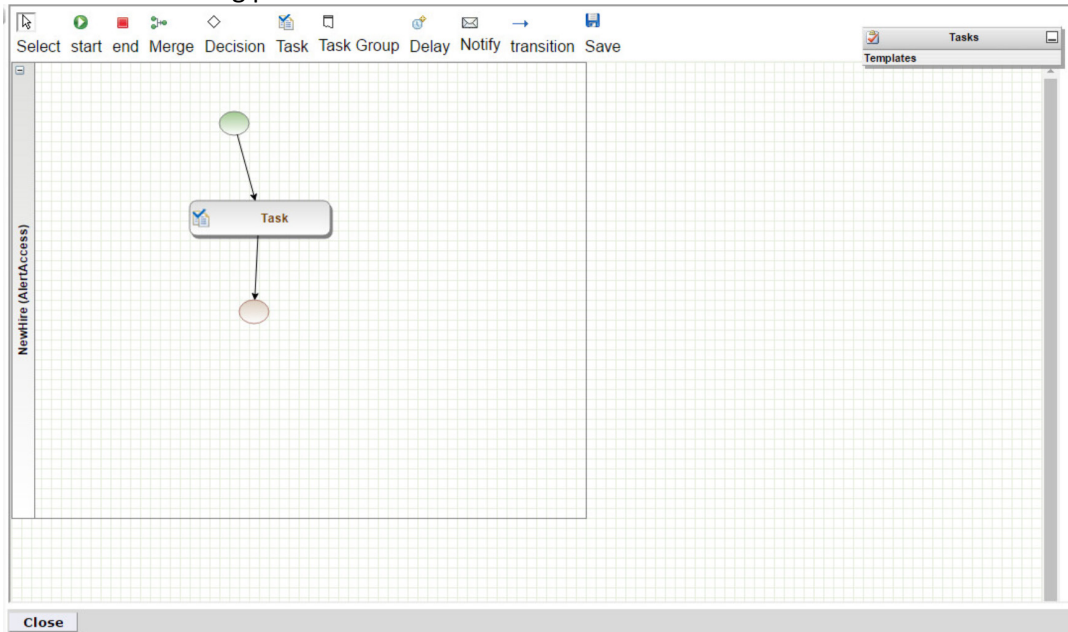
- 565 1. Navigate to **Setup>Manual Configuration>User Data>User Data Source**.
- 566 2. Click **New**. Create the following User Data Source:

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

567 2.1.16 Process Designer

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

571 4. Create the following process:



572

573 **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-Access 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**

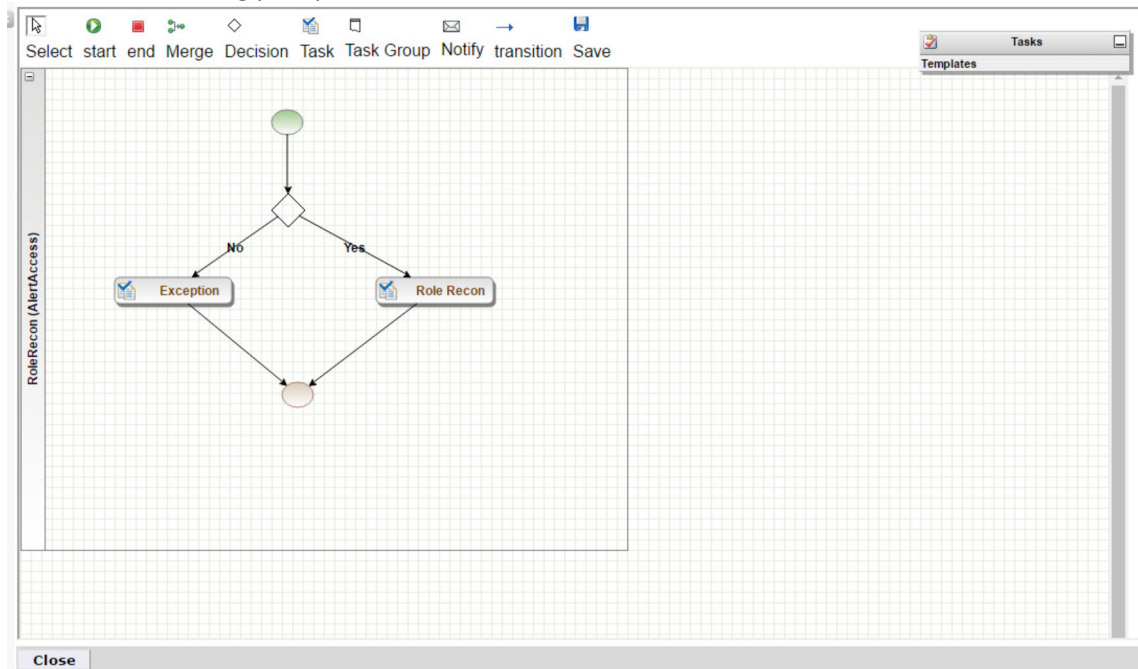
- 581 1. Navigate to **Setup>Manual Configuration>Policy Engine>Suggest/Default Access**.
- 582 2. Click **New**. Create the following criteria:

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

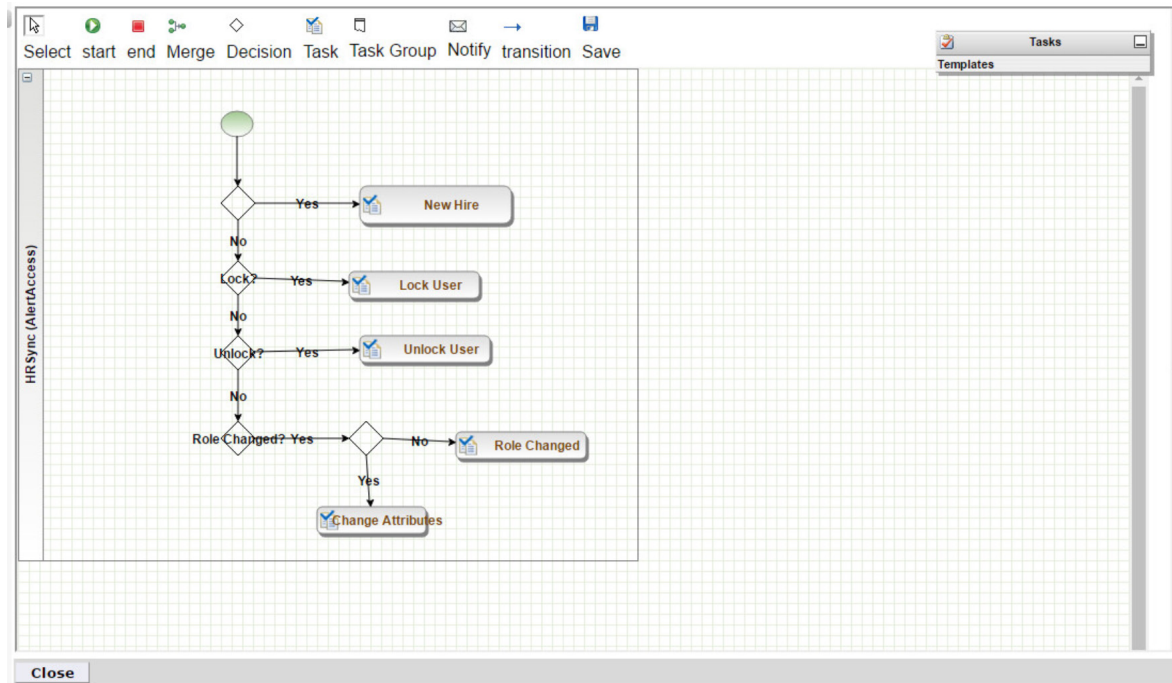
583 **2.1.19 Policy Designer**

- 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:

600

Group Name	Type
HR Sync	Reconciliation

601

2.1.21 Form Customization

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

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

604 *Note:* This list is not exhaustive. The application is deployed with several attributes preconfigured.605

2.1.22 User Field Mapping

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

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

Email	No	No	7
ManagerId	No	No	8
Department	No	No	9
JobTitle	No	No	10
CompanyName	No	No	11
ManagerName	No	No	12
FullName	No	No	13
Mobile	No	No	14
User Base Dn	No	No	15
ADUserId	No	No	16
LDAPUserId	No	No	17
ADUserName	No	No	18
LDAPUserName	No	No	19
EmployeeNo	No	No	20
Initials	No	No	21
Pager	No	No	22
L	No	No	23
Racfid	No	No	24
Racprogrammername	No	No	25
Racworkattrusername	No	No	26
Racaddressline1	No	No	27
Racaddressline4	No	No	28

610 **2.1.23 Provisioning Mapping**

- 611 1. Navigate to **Setup>Manual Configuration>Identity & Access>Provisioning>Provisioning**
- 612 **Mapping.**
- 613 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

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

616 **AD**

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

617 **RACF_OPENLDAP**

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

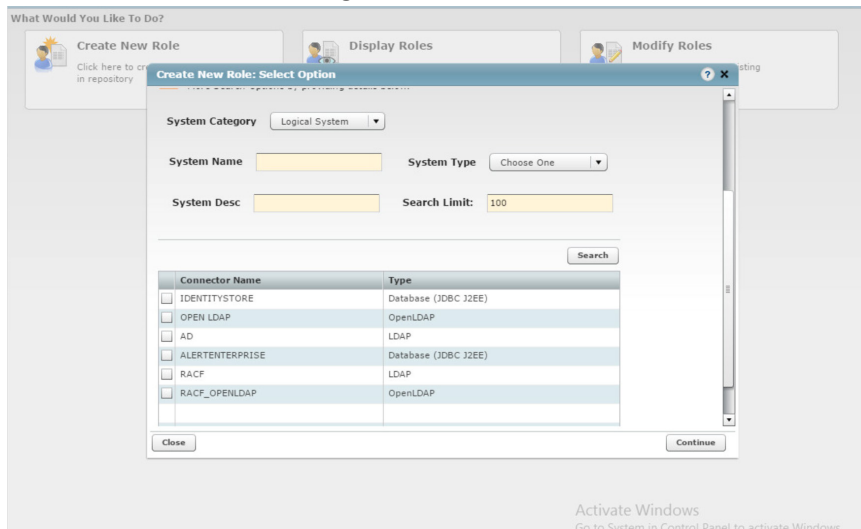
Name	Description
loginShell	loginShell

623 **RACF_OPENLDAP**

Name	Description
Racfid	Racfid
Racworkattrusername	Racworkattrusername
UserBaseDn	UserBaseDn
objectClass	objectClass
Racfprogrammerna me	Racfprogrammerna me
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.**
 630

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:

Description:

Resource Type: LDAP,OpenLDAP

Resource(s): AD OPEN LDAP

[Edit Resources](#)

Steps

1. Attributes 2. Process 3. Owners 4. Risk

5. Certification

Previous Step Next Step

1 Attributes

Role Comments Ma...

Role Hex Code:

* Alias:

Criticality:

Long Description:

Team Rooms:

Functional Area:

Location:

Process:

Alias1:

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

* Alias:

Criticality:

Long Description:

Status:

EvaluateForOthers:

Role Comments Ma...

Keywords:

UME User Group:

Role Sub Type:

Location:

Process:

Alias1:

Sub Process:

Role Comments Ma...

Admin Full Name:

Technical Role Na...

Role Stage:

Active for Provisioning:

Provisioning Assigned:

Previous Step Next Step

634 8. Create the following roles in the repository:

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

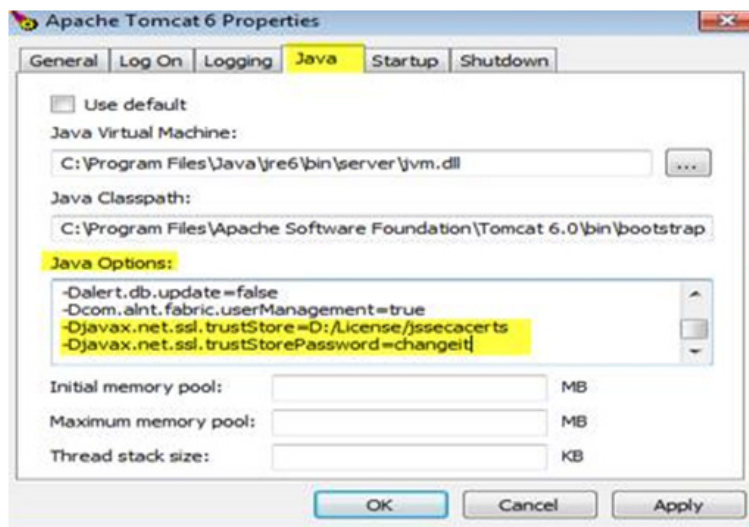
636 2.1.26 Enabling SSL

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:
 644 `cd D:\cert\`
- 645 4. Download certificate from directory server using the following command:
 646 `java -cp ALNTADCertUtil.jar com.alnt.ADCertInstaller`
 647 `<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`
 650 `-Djavax.net.ssl.trustStore=D:/License/jssecacerts`
 651 `-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
 - 713 VLANs).
- 714
 - For Directory Service mode authentication, setup of Microsoft Active Directory (AD) with an AD
 - 715 Service Account and the recommended HyTrust security groups, as described in the *HyTrust*
 - 716 *CloudControl Administration Guide*.
- 717
 - 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
- 725 Pa\$\$wOrd123!.
- 726 2. You are prompted to assign a new password to the local HTCC administrator account
- 727 (*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
- 730 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:~ dwyne$ 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:

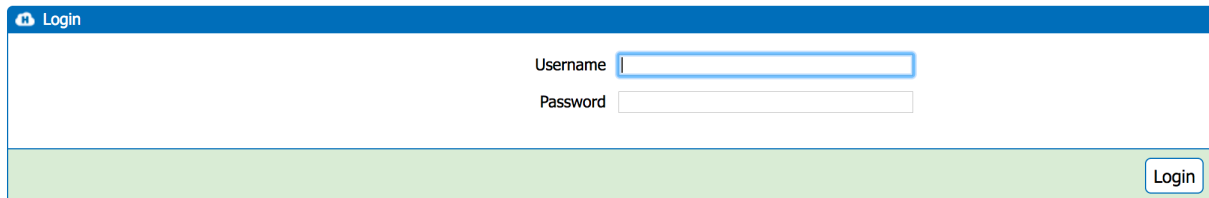
      IP: 192.168.20.11
      Netmask: 255.255.255.0
      Gateway: 192.168.20.1
      DNS Server: 192.168.19.10

```

- 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.

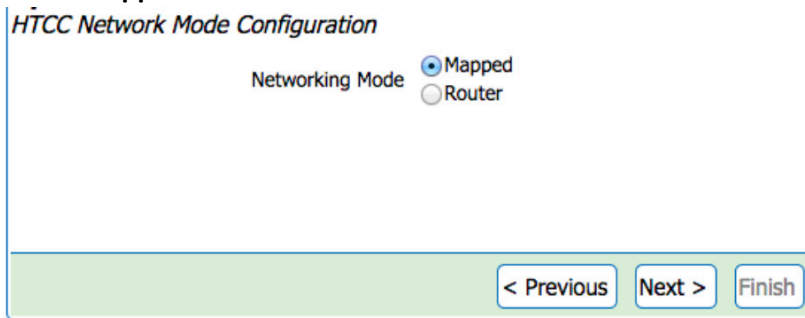
740 The login screen appears.



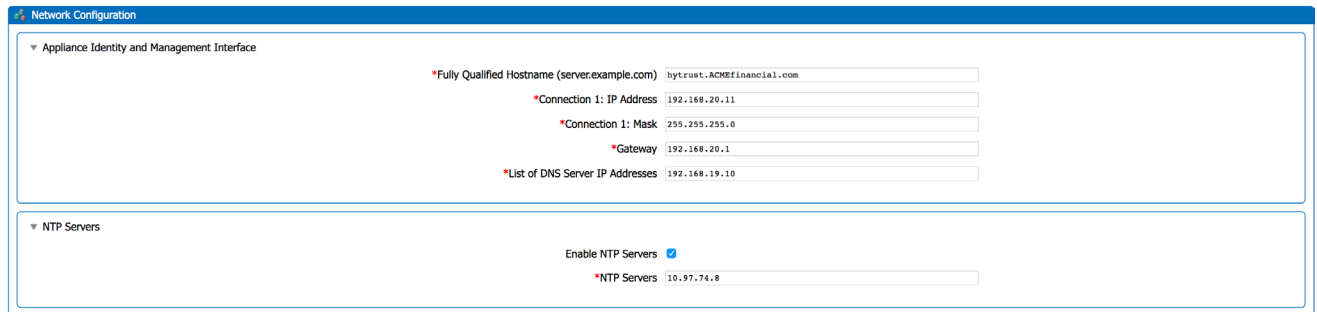
- 741
- 742 Once logged in, you can complete the initial setup and configuration. Here is an overview of the initial
- 743 setup and configuration steps. The detailed steps can be found in the HTCC installation guide, which is
- 744 available on request.
- 745 1. Accept the end-user license agreement.
- 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:**

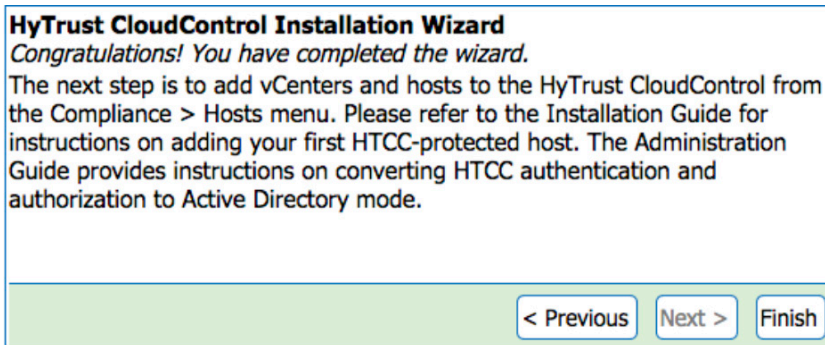
- 750 1. Select **Mapped** as the HTCC Network Mode



- 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
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

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

- 761
762 ESXi:

*Friendly Name
Description
*Hostname/IP

Host Type

Protected

Managed

Labels

763 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

Description

*Hostname/IP

User ID

Password

Host Type

Protected

768

*HTTPS Secure Port

Use HTTPS Secure Port

*HTTP Port

Use VI SDK Secure Port

*VI SDK Port

*VI SDK Secure Port

Logging Aggregation Local
 Explicit Syslog Server

Syslog Server

Authentication Mode Use HTCC Service Account (default)

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

769

*Published Hostname/IP

*Published IP Mask

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

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.

*Published Hostname/IP

*Published IP Mask

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.

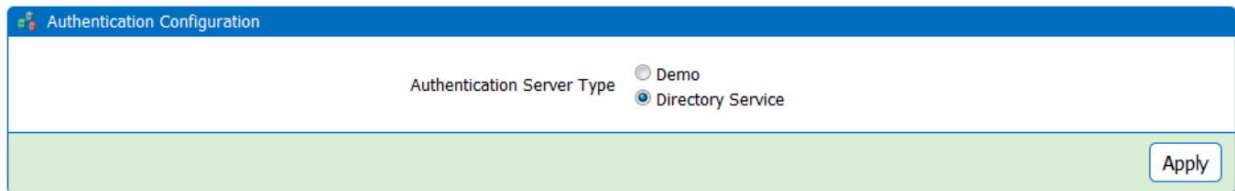
- Domain object: *Read memberOf*
- User object: attributes *memberOf* and *distinguishedName*
- Group object: attributes *member*, *memberOf*, and *distinguishedName*

To convert HTCC to Directory Service mode:

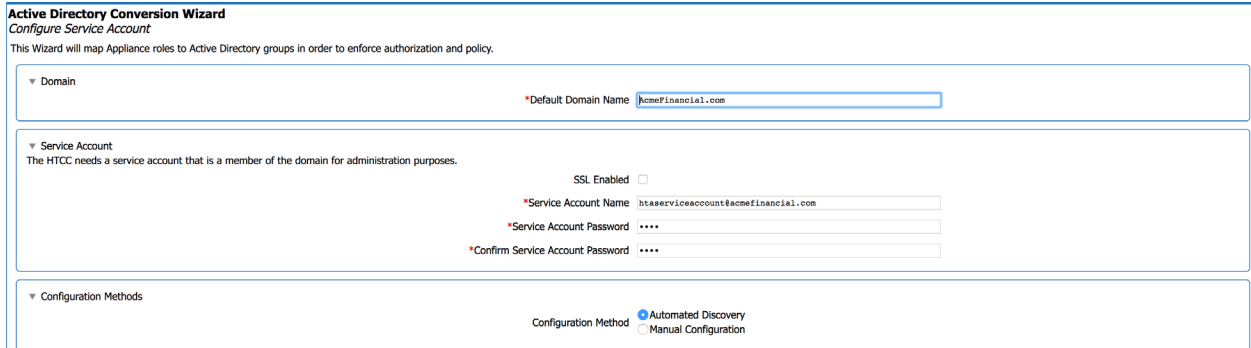
1. Open the Authentication Configuration page (**Configuration > Authentication**).

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

Configuration > Authentication Configuration

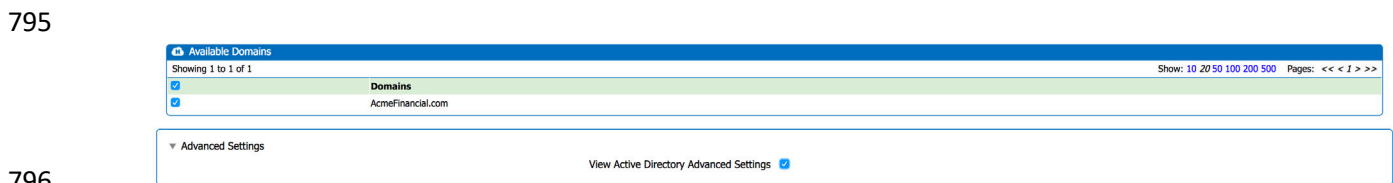


788 The Active Directory Conversion Wizard opens, which guides you through the steps to connect HTCC
 789 to your directory service. The first page is the Configure Service Account page.
 790

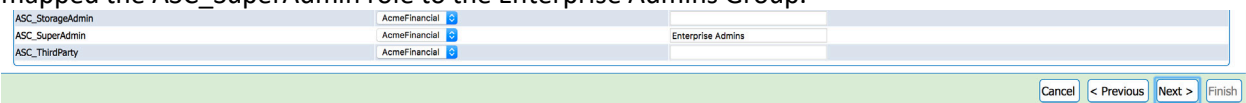


791 3. Use the Service Account panel to specify the AD HTCC service account information. Select **Auto-**
 792 **matized Discovery**. Click **Next**.
 793

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



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



799
 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 Us-
- 808 *ers*' 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.

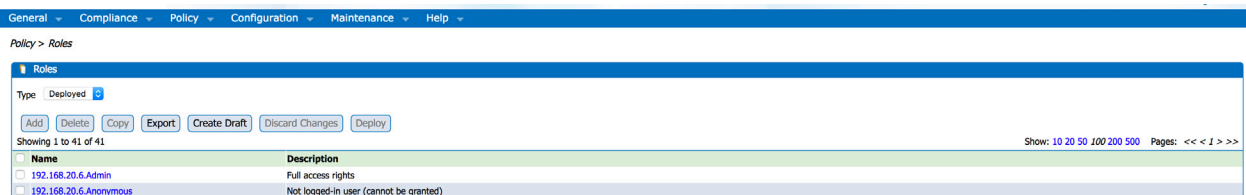
818 Any time a new virtual machine is created or a new host is added, the new object is automatically added
819 to the HTCC policy and the deployed policy is enforced on the new object. To view the current policy,
820 navigate to **Policy>Resources**. The *Deployed* policy is the policy that is currently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

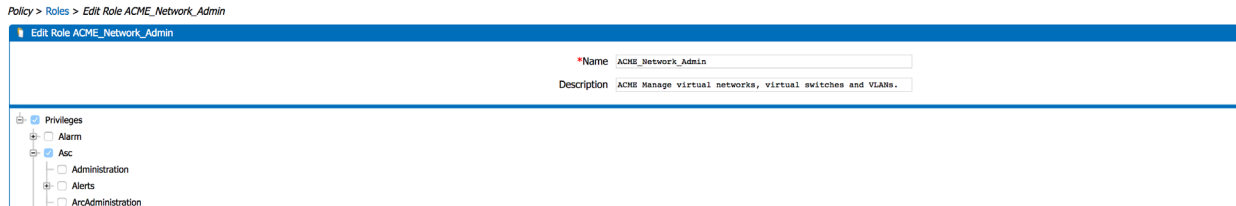
- 823 1. Open any **Policy** page.
- 824 2. Click the **Create Draft** button. This copies the "Deployed" policy to a "Draft" policy.
- 825 3. Make your desired changes to the Draft policy using the various policy pages.
- 826 4. Click the **Deploy** button to replace the current Deployed policy with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



- 832 3. Select **Add**. First, create the network admin role. Then, name the role and provide a description.
- 833

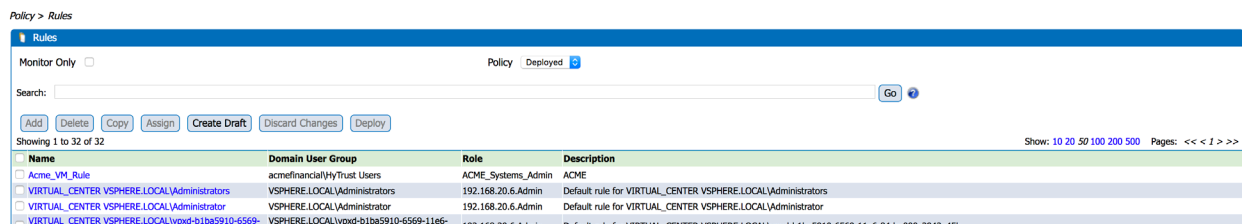


- 834
- 835 4. Select all of the following permissions:
- 836 a. **Asc>NxOsConfig, NxOsShow, NxOsXmlApi,ssh,storage**
- 837 b. **DVPortgroup>Entire List** (*Note: This configuration item is deprecated in versions 5.1 and*
- 838 *above of the product.*)
- 839 c. **DVSwitch>Entire List**
- 840 d. **DataCenter>IpPoolConfig,IpPoolQueryAllocations,IpPoolReleaseIp**
- 841 e. **Global>CancelTask,LogEvent**
- 842 f. **Host>Config>AdvancedConfig,NetService,Network,PciPassthru**
- 843 g. **Network>Assign,Delete,Router**
- 844 h. **Resource>Delete**
- 845 i. **System>Entire List**
- 846 j. **Task>Entire List**
- 847 k. **VirtualMachine>Config>ManagedBy,MultiActions**
- 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**

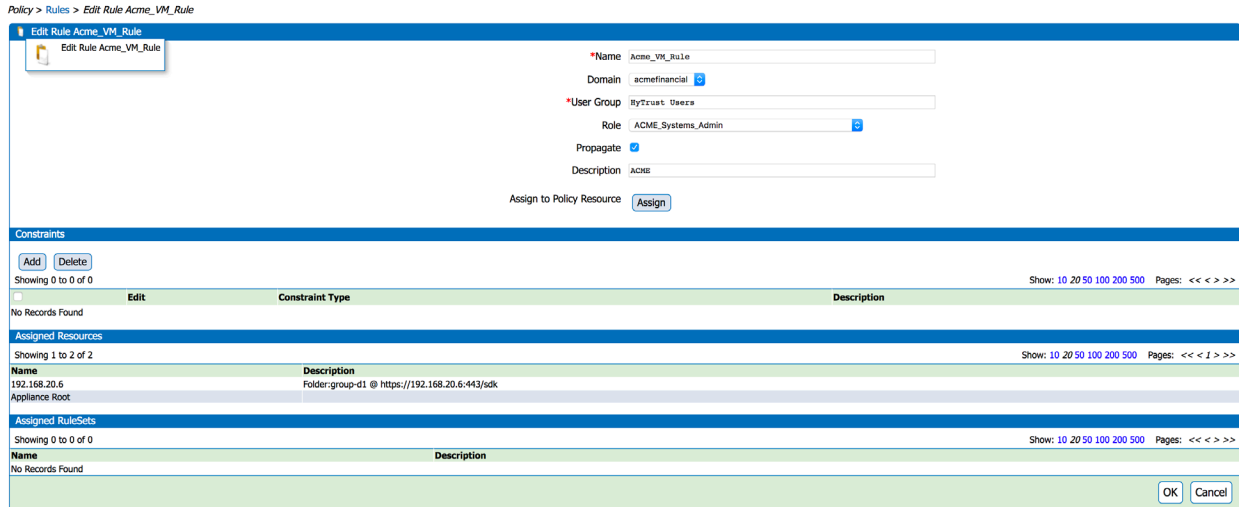
856 Next, you must create the rules that will apply the roles to the host. First, create the rule for the system

857 admins role, assigning it to the 'HyTrust Users' AD group.

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

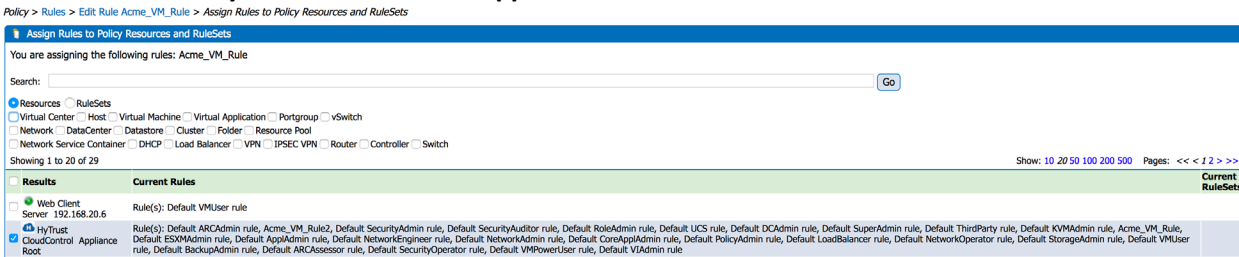


- 860
- 861 10. Select **Add**. Name the rule and type in the user group created in Active Directory.



862
863
864

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



865
866
867
868
869
870

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

871 2.2.9 Configure Logging

- 872 1. Select **Configuration > Logging**.
- 873 2. Select the **DEBUG** logging level.
- 874 3. Select **External**.
- 875 4. Select **CEF**.

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

Configuration > Logging Configuration

Logging Configuration

HTCC Logging Configuration

Logging Level DEBUG

HTCC Logging Aggregation Local External

Logging Aggregation Template Type Proprietary CEF

*HTCC Syslog Servers 192.168.17.10:514

Encrypt Syslog

Manage Logs

Repair Log

Log Viewer

Host Default Logging Configuration

Default Logging Aggregation Local Explicit Syslog Server

*Default Syslog Server 192.168.17.10:514

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-](https://technet.microsoft.com/en-us/windows-server-docs/identity/ad-ds/deploy/install-a-new-windows-server-2012-active-directory-forest--level-200-)
 906 [windows-server-2012-active-directory-forest--level-200-](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
 913 set up at: https://www.splunk.com/page/sign_up

914 Download the Splunk Universal Forwarder from: [http://www.splunk.com/en_us/download/universal-](http://www.splunk.com/en_us/download/universal-forwarder.html)
 915 [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,
 917 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

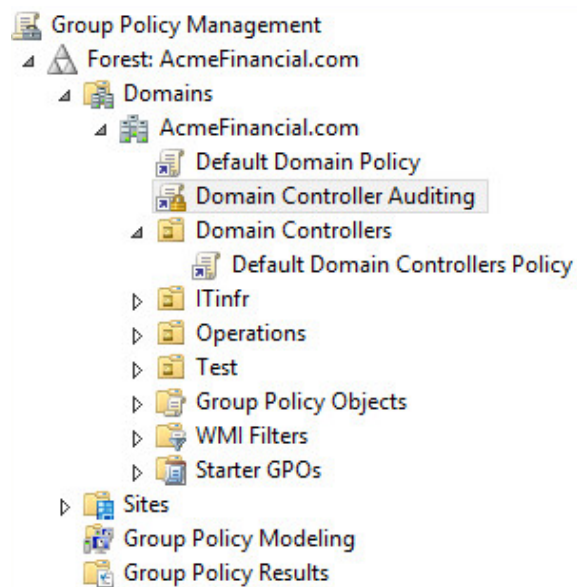
919 Install Microsoft Security Compliance Manager: [https://www.microsoft.com/en-](https://www.microsoft.com/en-us/download/details.aspx?id=53353)
 920 [us/download/details.aspx?id=53353](https://www.microsoft.com/en-us/download/details.aspx?id=53353)

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:



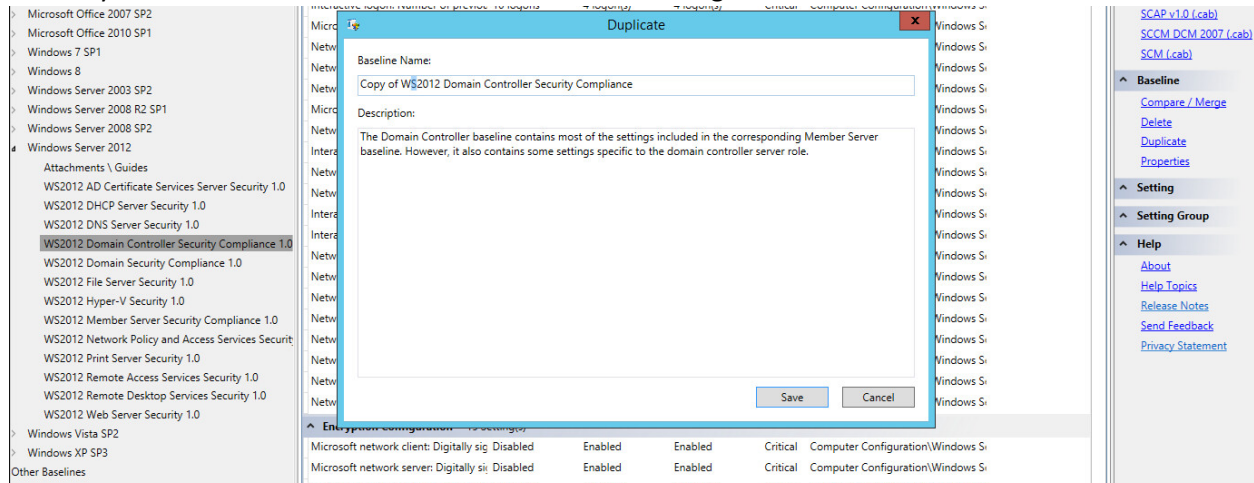
932

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*.”

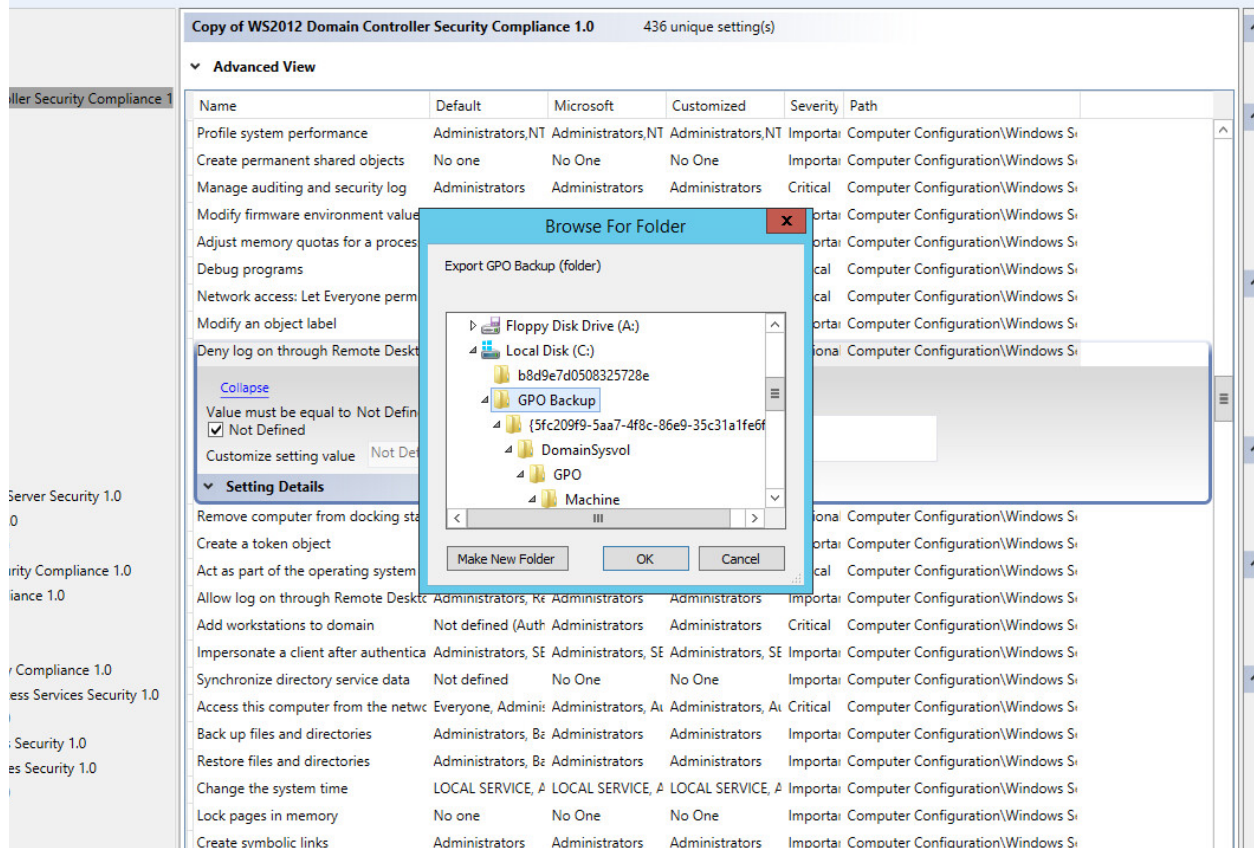
935 Minor changes are made to the Domain Controller Auditing Policy to enable the ability to audit user
 936 account changes, attribute changes, and policy changes for this build.

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.



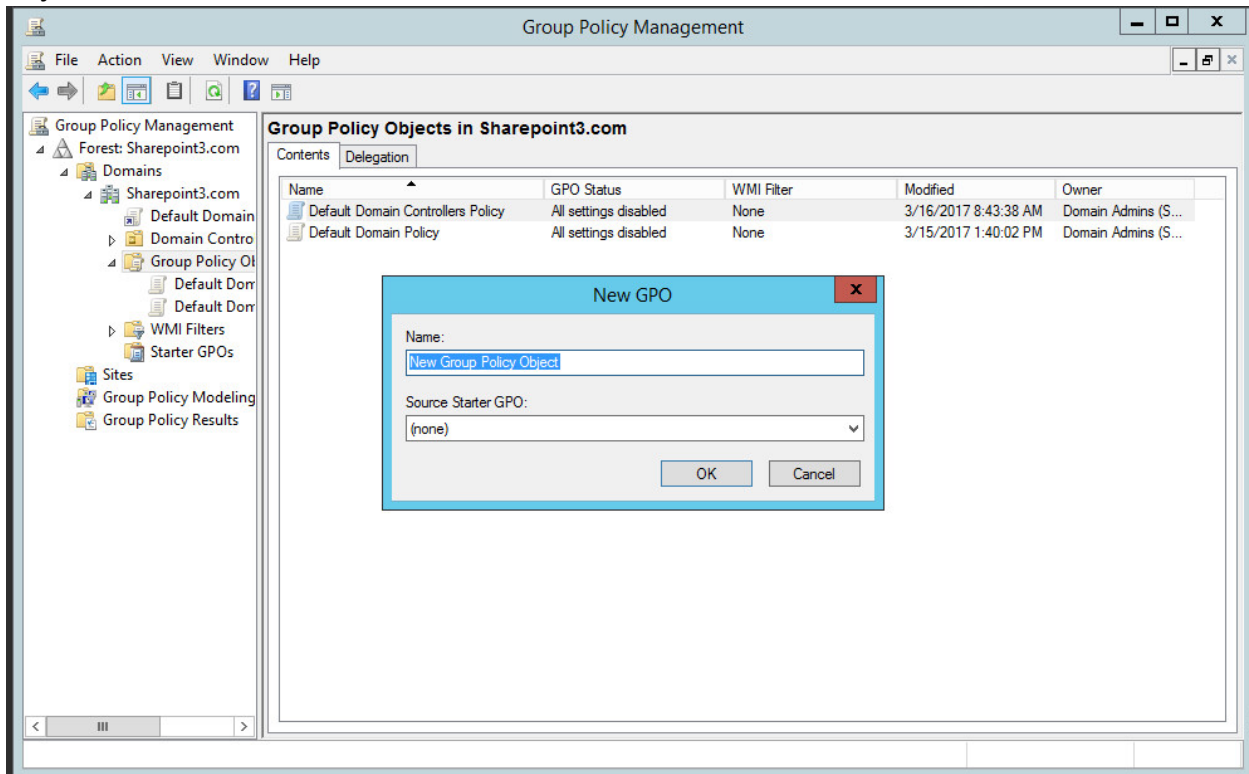
941 2. Export to a GPO backup folder.
942



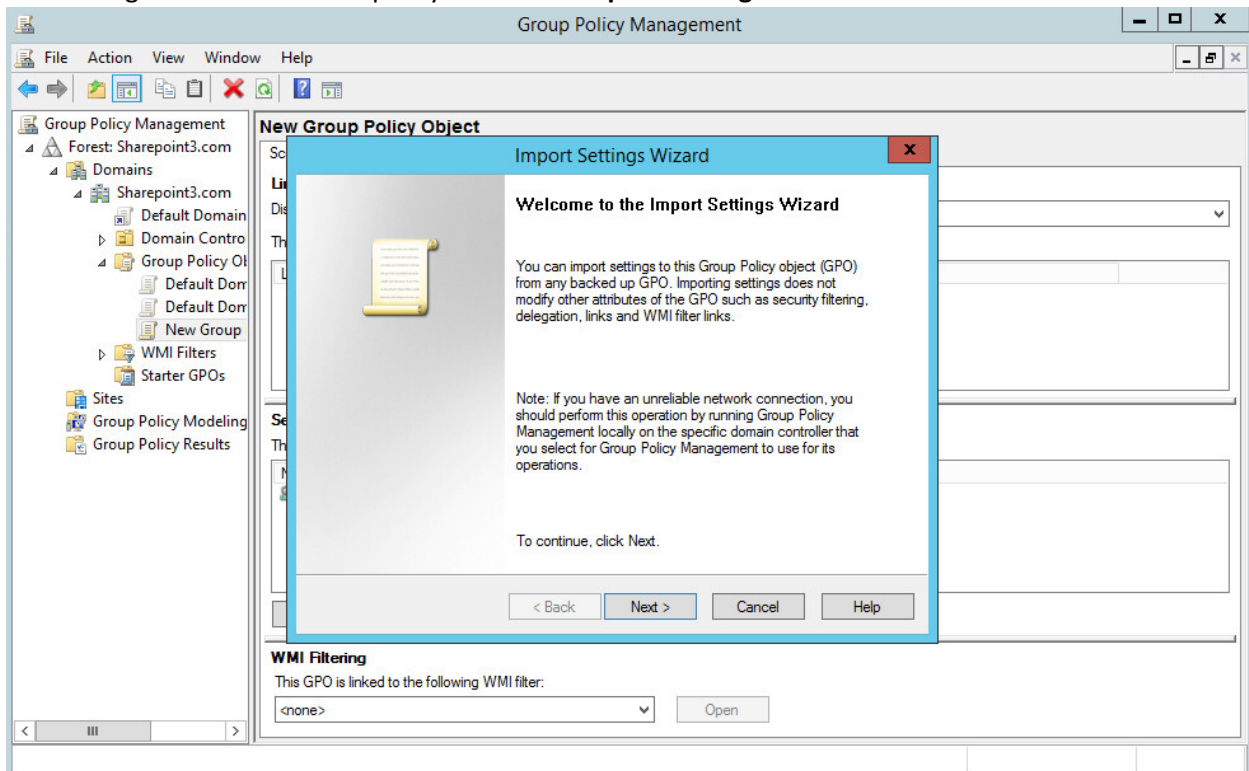
943

DRAFT

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

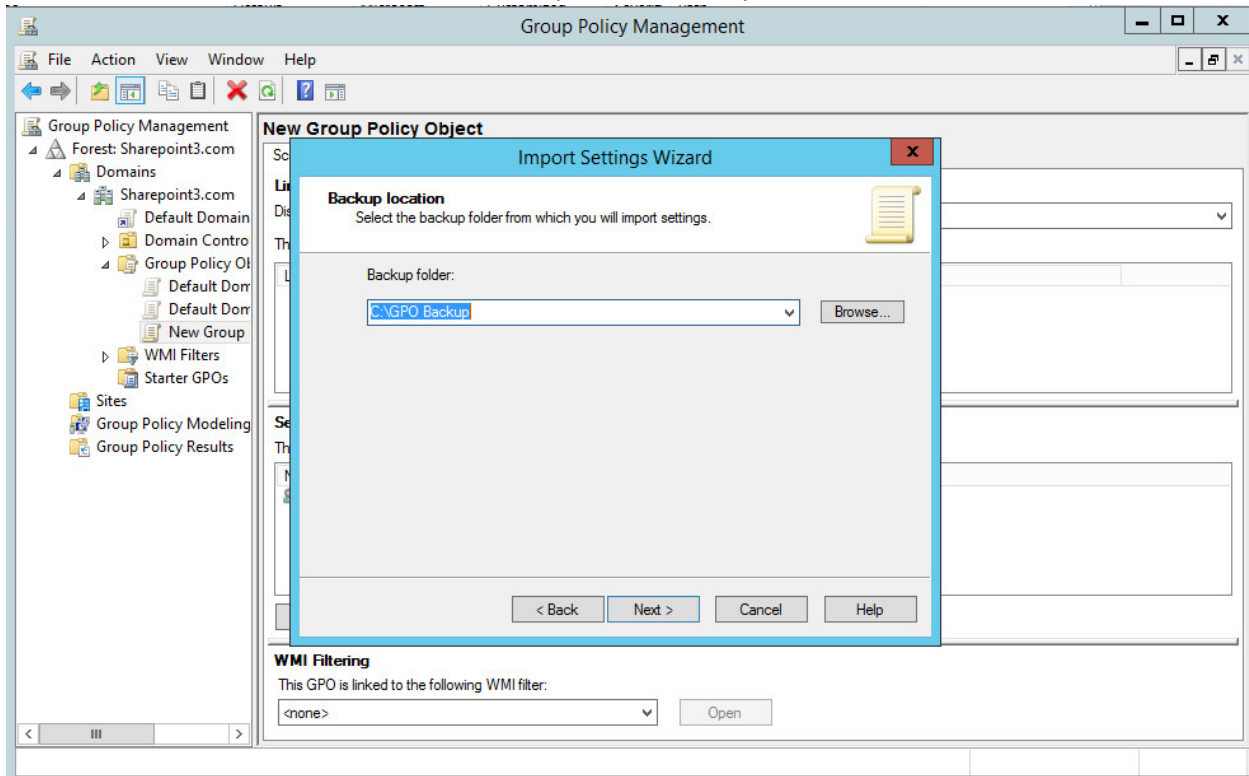


- 946 4. Right-click on the new policy and select **Import Settings**. Click **Next**.
947

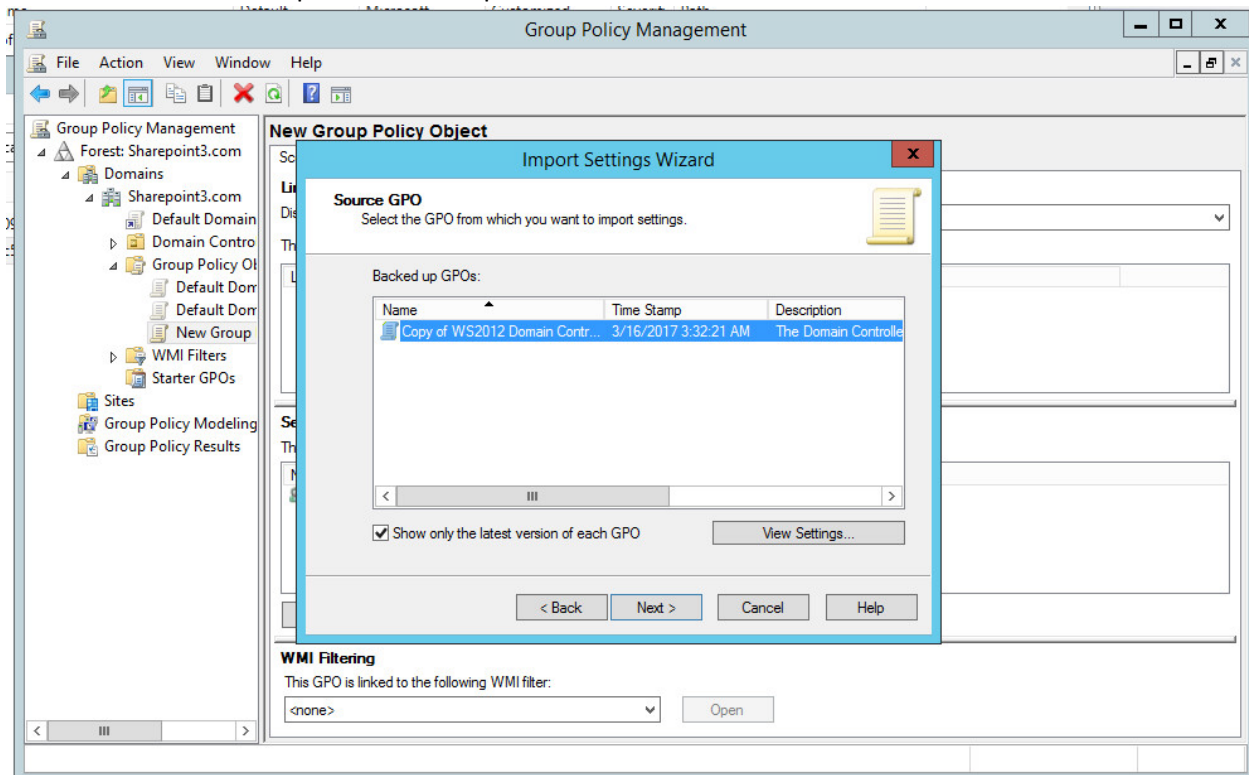


948

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

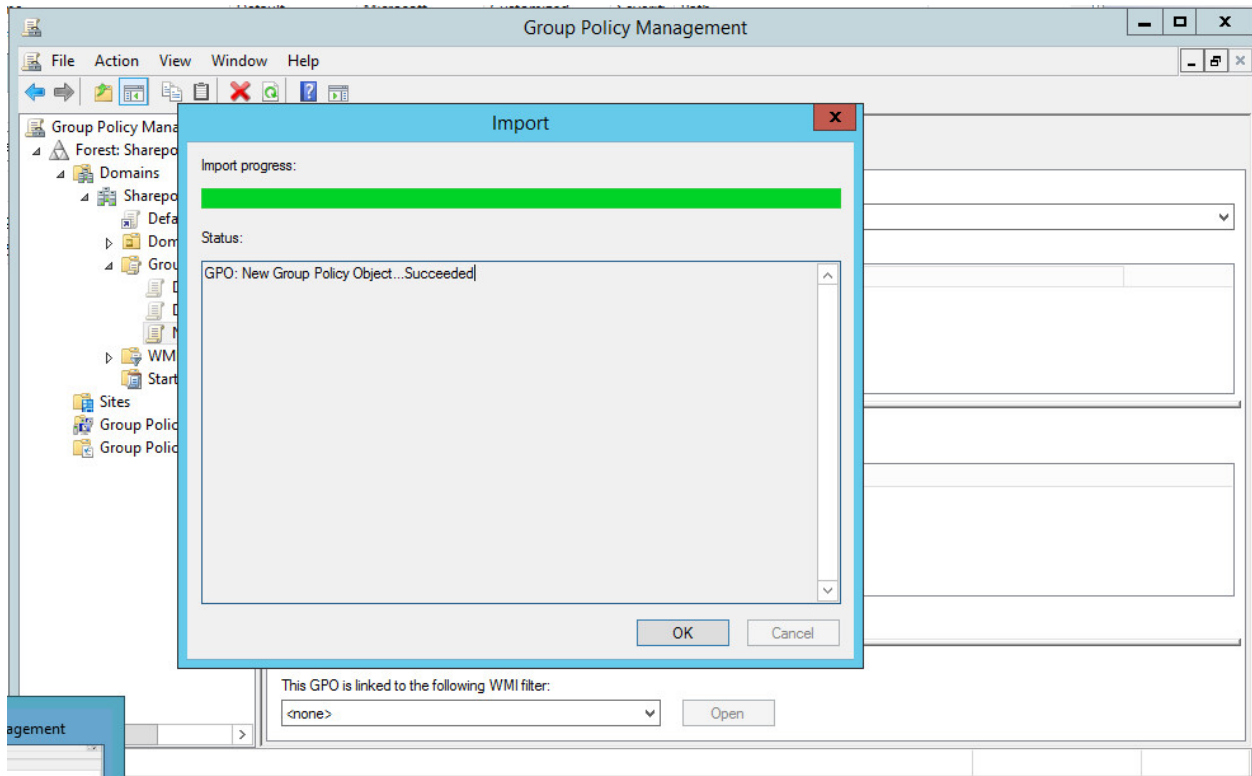


950 951 6. Select the backup created in Step 2.

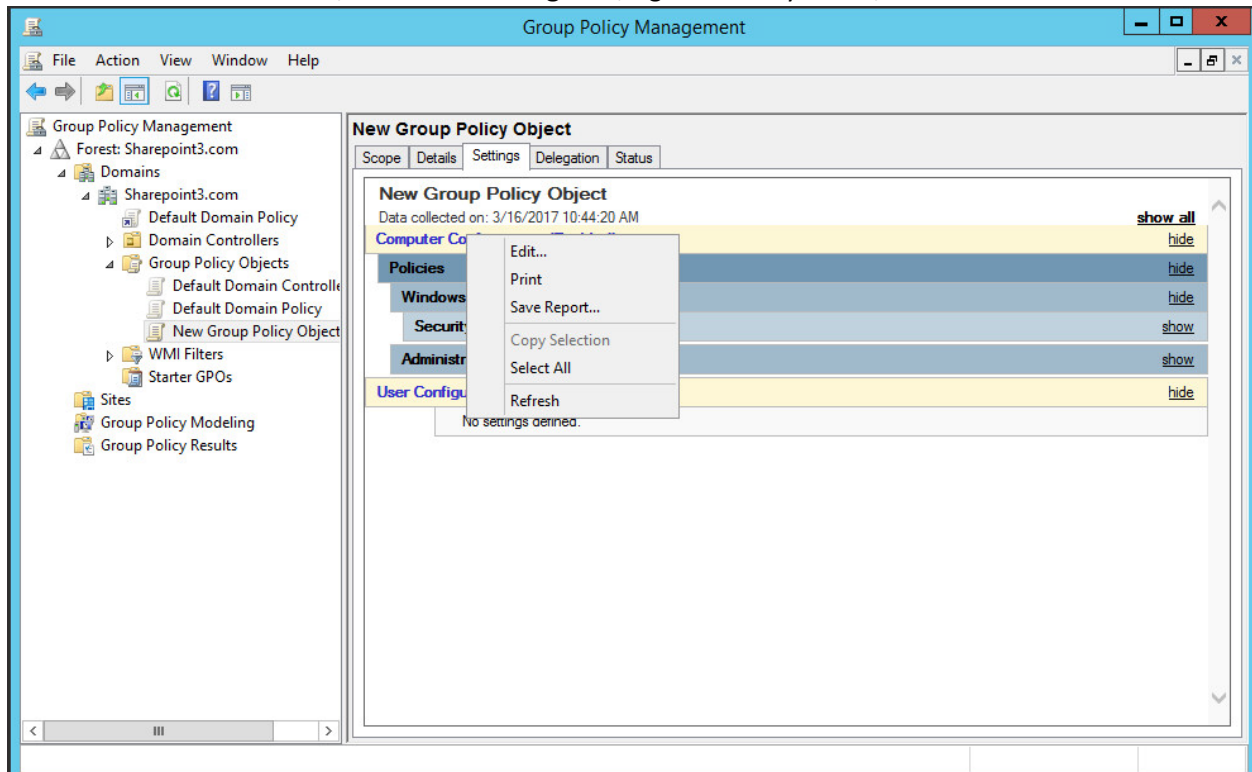


952

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

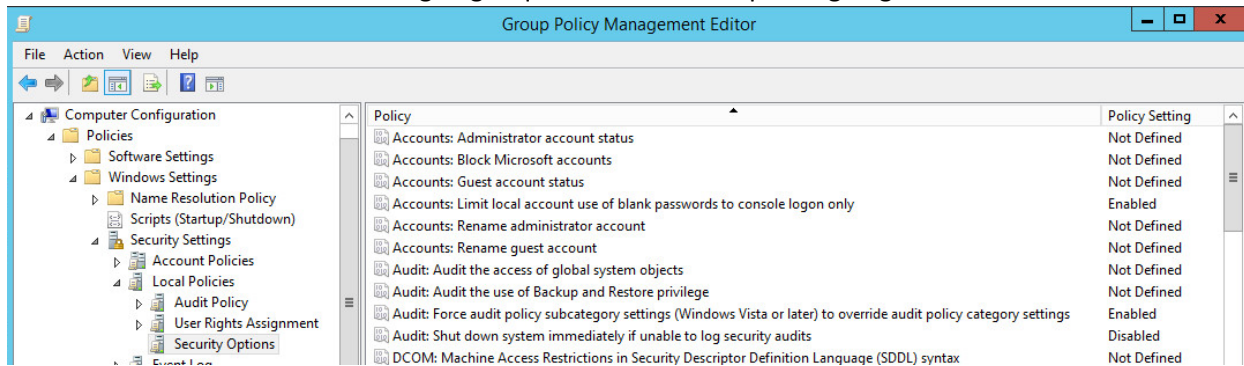


954 8. Select the new GPO, select the **Settings** tab, right-click anywhere, and select **Edit**.



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

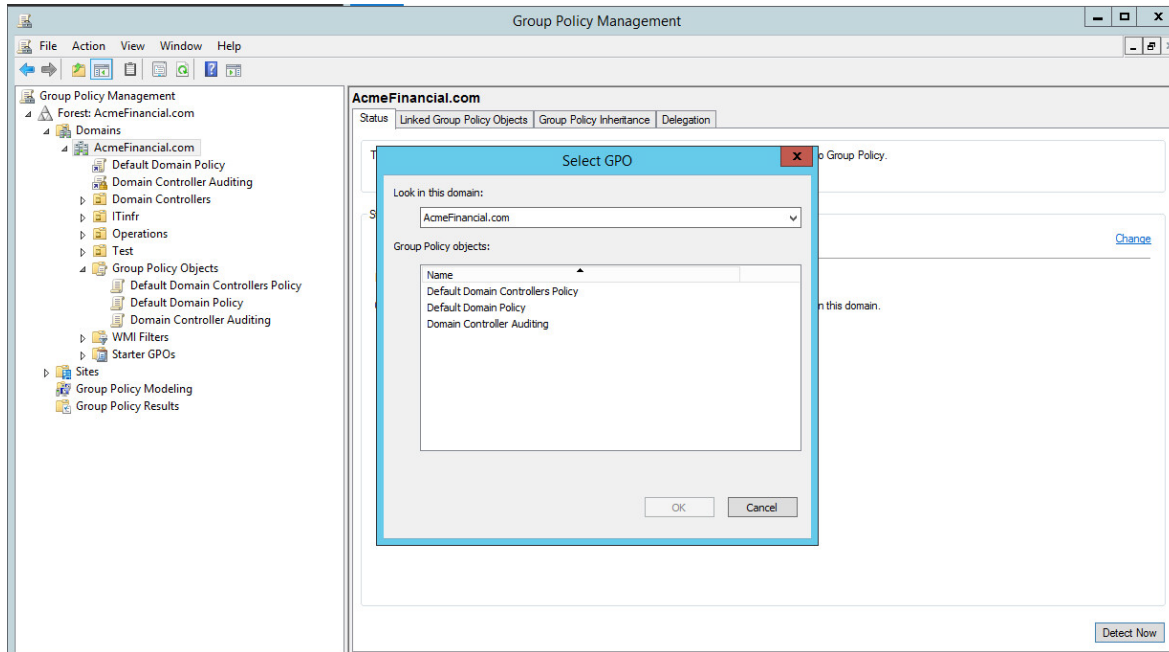
959 (Windows Vista or later) to override audit policy category settings” to “Enabled.” Change the value for
 960 “Domain controller: LDAP server signing requirements” to “require signing.”



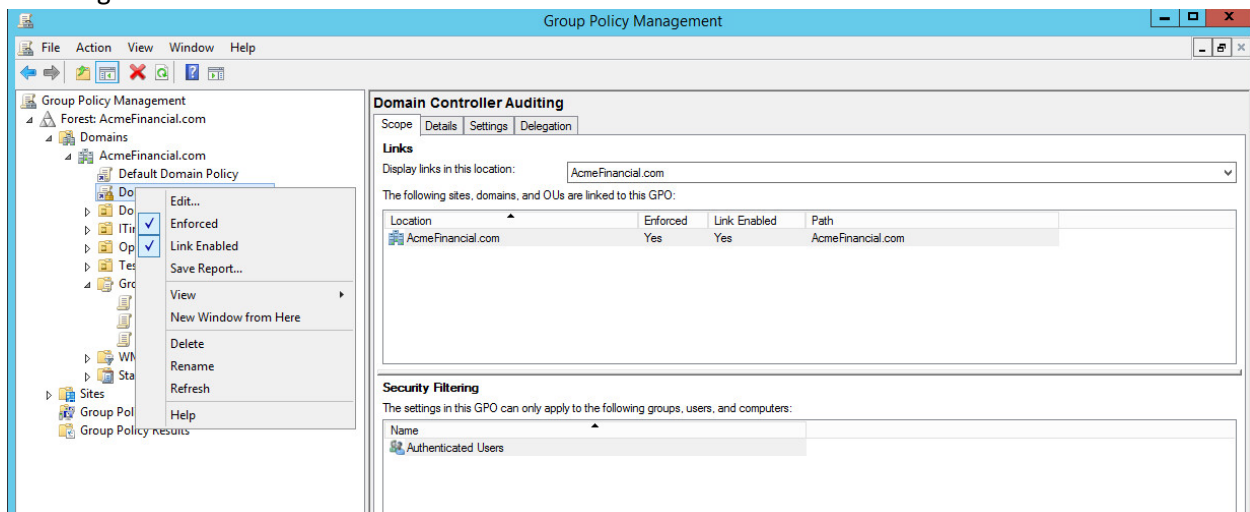
961
 962 10. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>Advanced**
 963 **Audit Policy Configuration>Audit Policies**. Make the following changes and save:

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

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

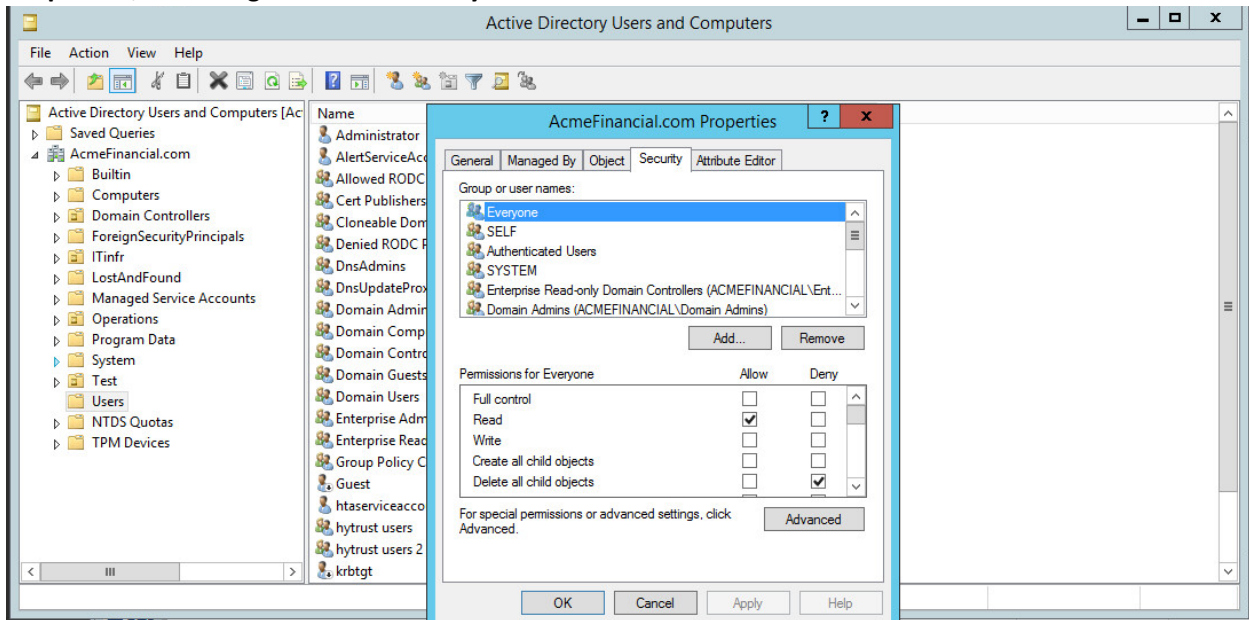


966 12. Right-click on the new GPO linked directly under the top-level domain and select **Enforced** by
967 checking it on the left.

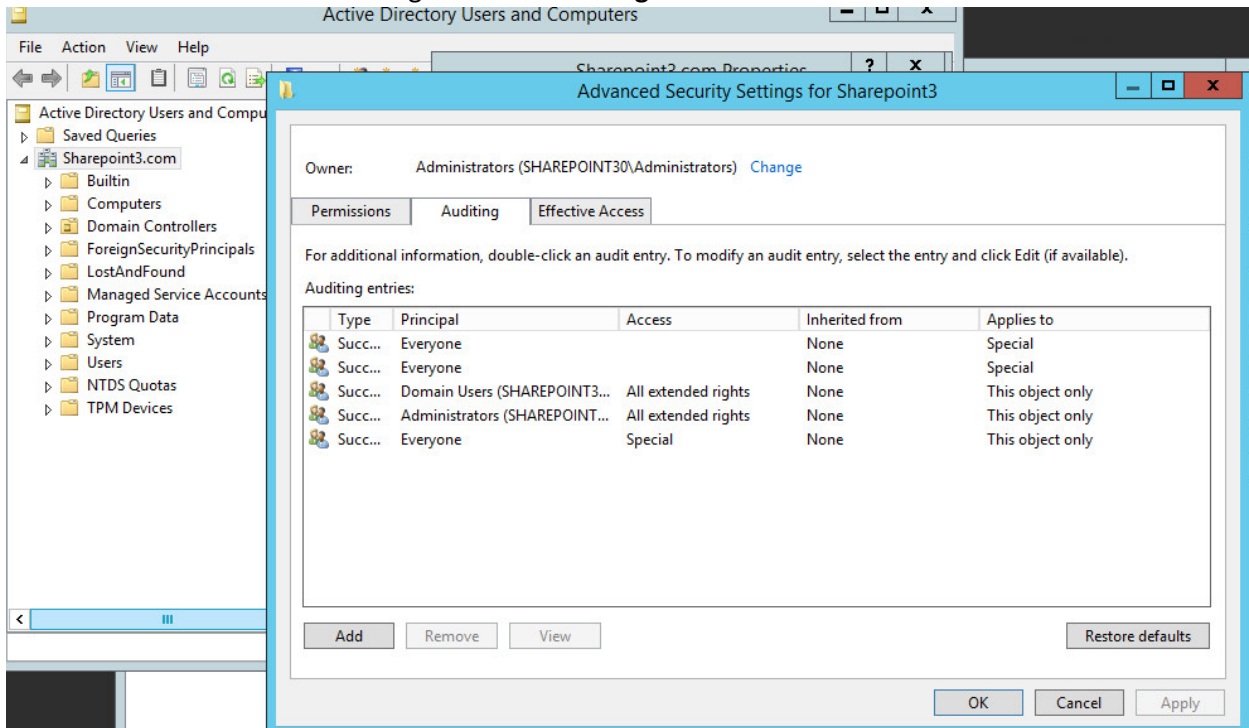


968

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.

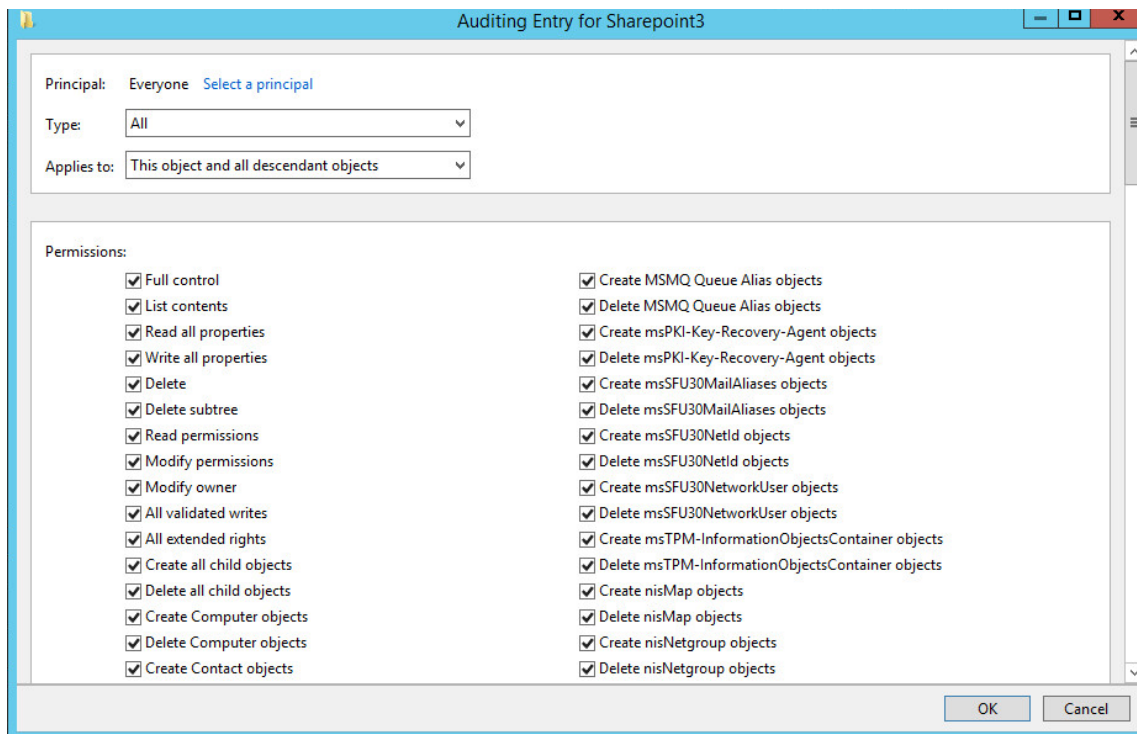


971 14. Select **Advanced** and navigate to the **Auditing** tab.
 972



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

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 yyy"
998     #Overwrite the contents of prevtime-file.txt with the current date
999     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > 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 yyy"
1015        Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > 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    }

```

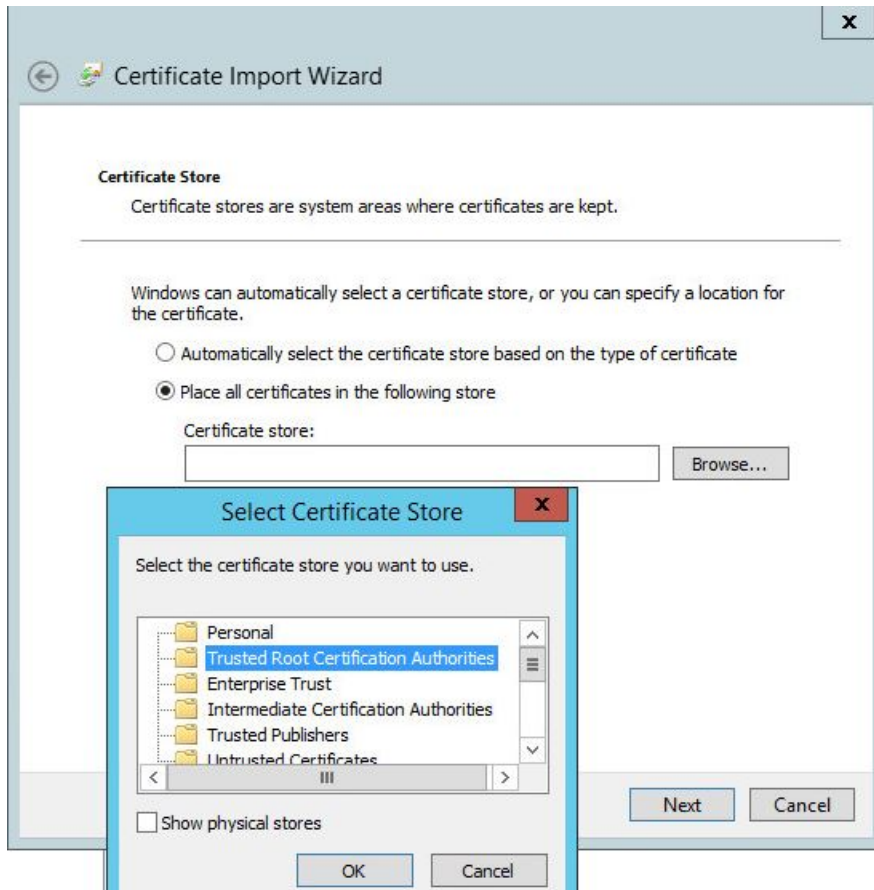
1021 2.3.9 LDAPS Configuration

1022 Once installed, the Active Directory service listens for both LDAP and LDAPS connections. To make
1023 LDAPS active, you will need to make sure that the certificates for the Active Directory domain controller
1024 and the certificate authority (CA) that signed the certificate are properly installed. Once these
1025 certificates are imported, LDAP clients will be able to use the LDAPS service.

- 1026 1. Copy the CA and domain controller certificates over to the Active Directory domain controller.
- 1027 2. Right-click on each certificate and choose **Install Certificate**.
- 1028 3. Choose **Local Machine**.



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



1037

1038 2.4 NextLabs Entitlement Manager

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

1041 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.

1047 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**

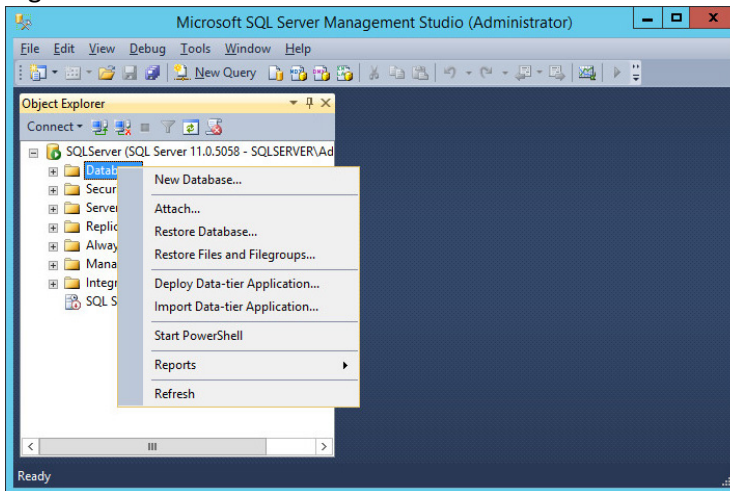
1063 NextLabs Control Center requires an Oracle or MS SQL Server. It is recommended that the database be
 1064 given 500GB of free storage space. In this build, only 100GB of storage is used for development
 1065 purposes.

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**

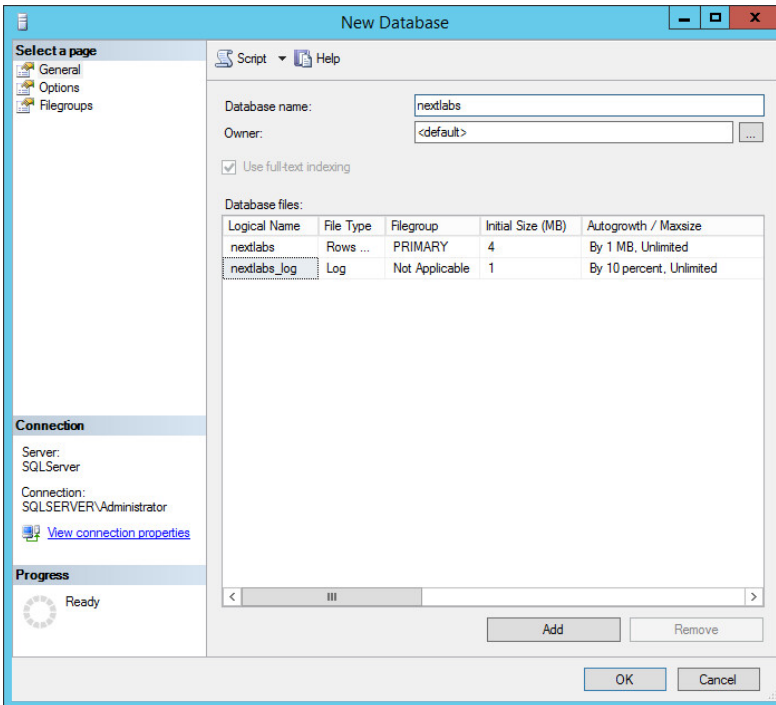
- 1072 1. Install the Microsoft SQL Server 2012 according to instructions available [online](#).
 1073 2. Open Microsoft SQL Server Management Studio and log in to the Microsoft SQL Server.
 1074 3. Right-click on **Databases** and left-click on **New Database**.



- 1075 4. In the New Database window, specify a **Database name** that works for you. The application au-
 1076 tomatically copies this into the **Logical Names** of the **Database files**. Click **OK**. Example name
 1077

1078

from this build: **nextlabs**.

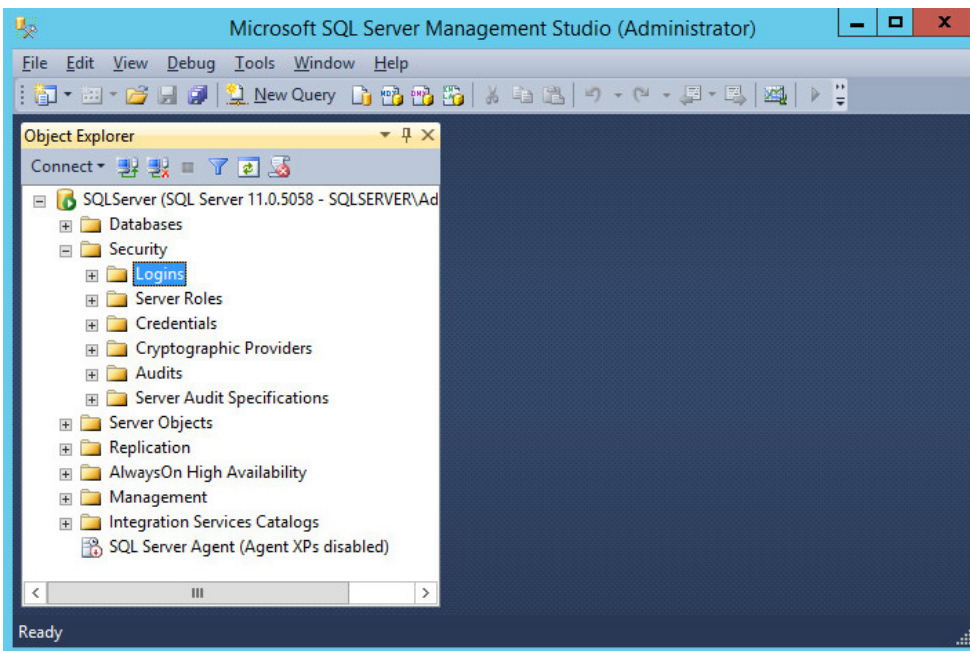


1079

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.

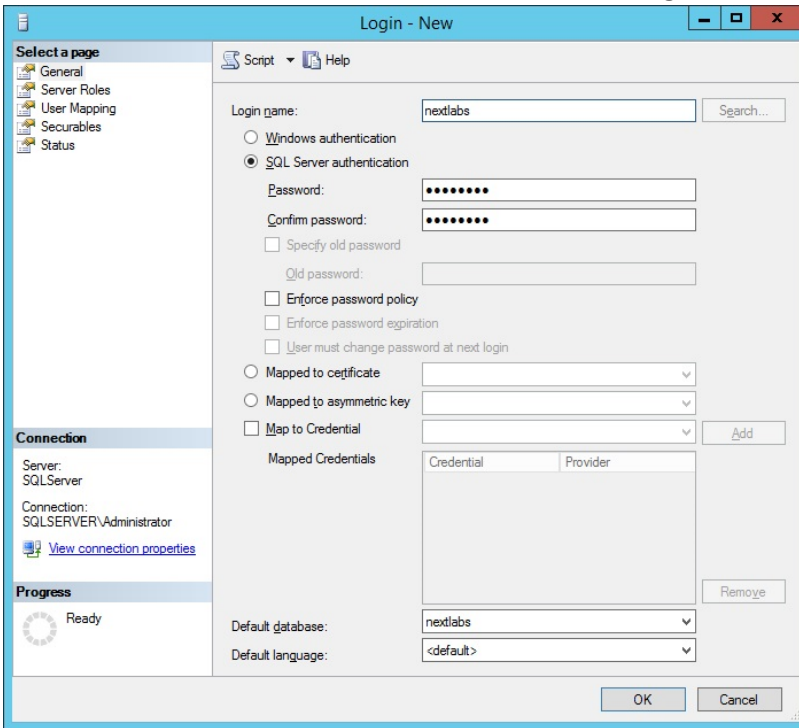


1082

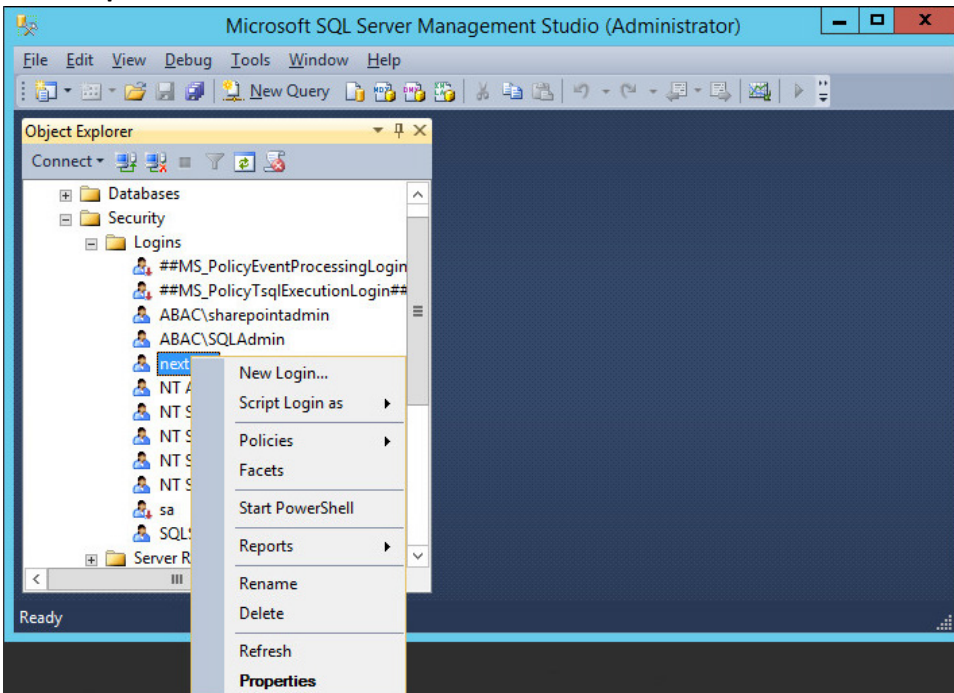
1083

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

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

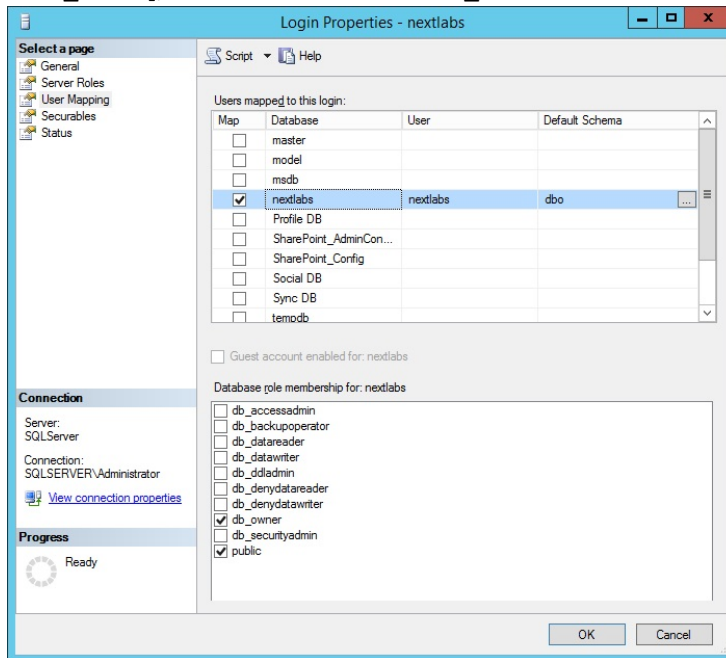


- 1085 8. Click the menu box next to **Logins**. Right-click on the new user created in the previous step.
1086 Click **Properties**.
1087

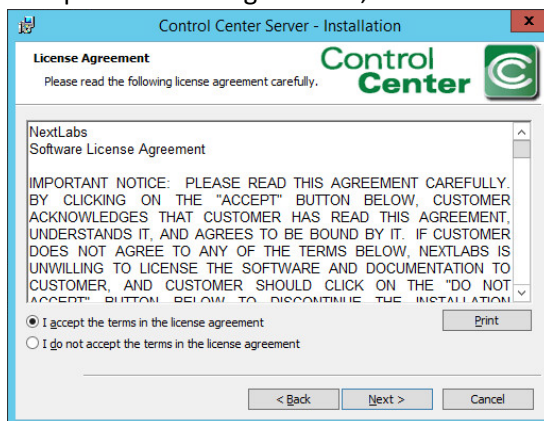


1088

- 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**.

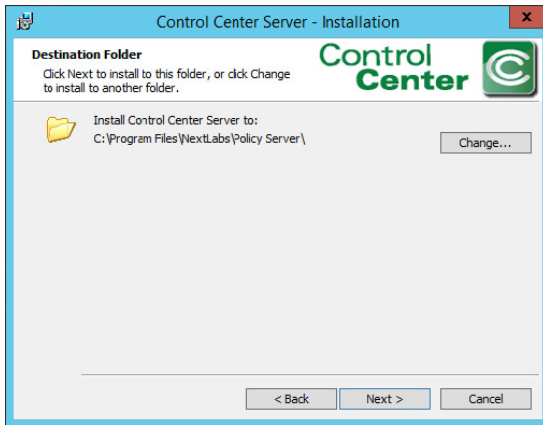


- 1091
 1092 10. Locate the installation zip file, provided by NextLabs support, and extract it.
 1093 11. Run the installer as follows:
 1094 a. On a Windows server, launch Command Prompt as Administrator.
 1095 b. In the command prompt, navigate to the folder that contains `install.bat`. The
 1096 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**.



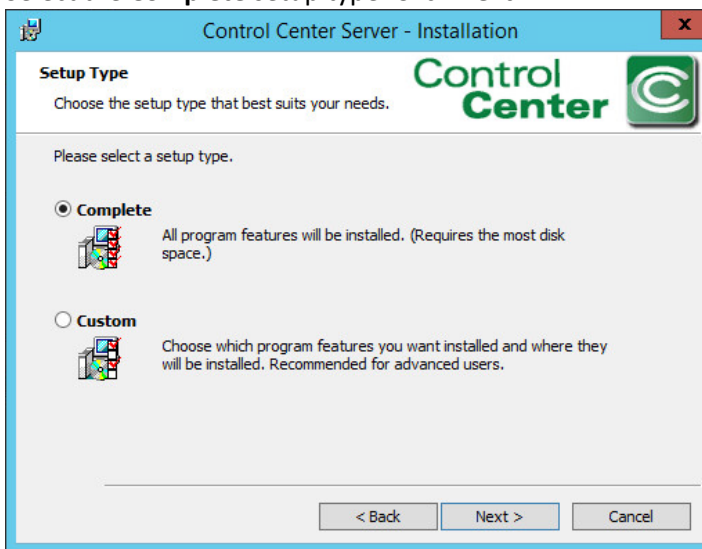
1101

1102 15. Click **Next**.



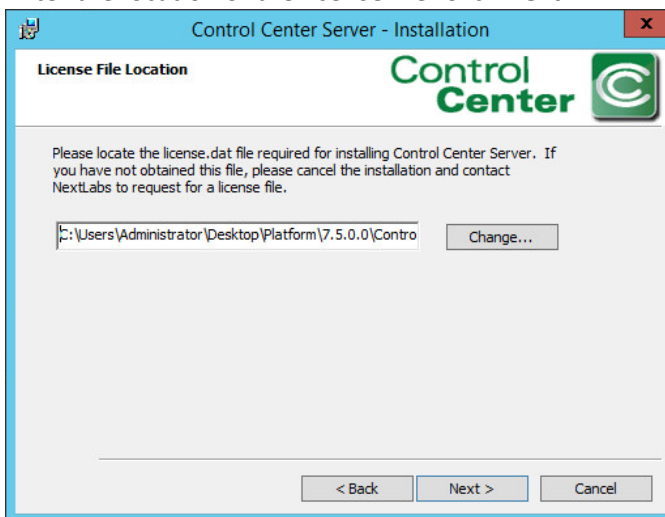
1103

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



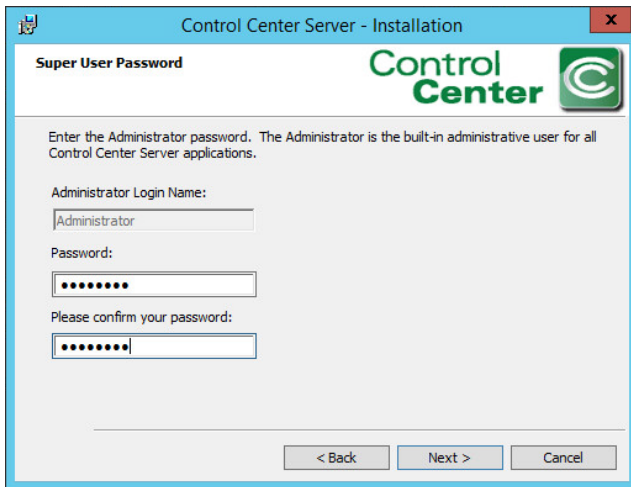
1105

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

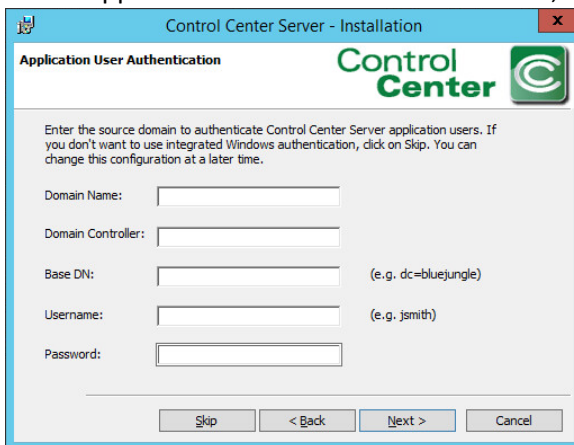


1107

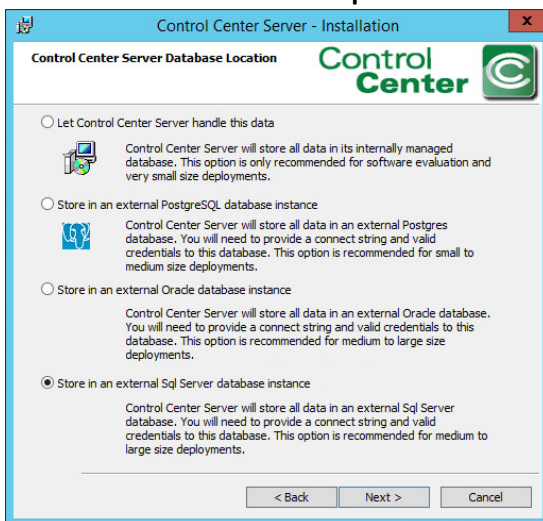
- 1108 18. Enter a Password for the built-in administrative user for all Control Center Server applications.
1109 Click **Next**.



- 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**.

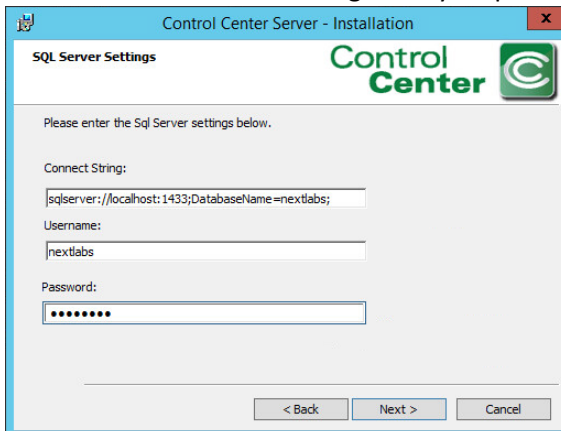


- 1114
1115 22. Select **Store in an external Sql Server database instance**. Click **Next**.



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.



Control Center Server - Installation

SQL Server Settings

Please enter the Sql Server settings below.

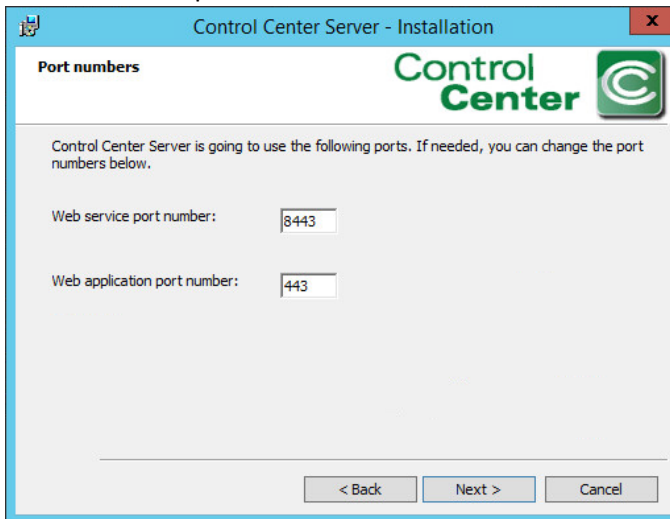
Connect String:

Username:

Password:

< Back Next > Cancel

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



Control Center Server - Installation

Port numbers

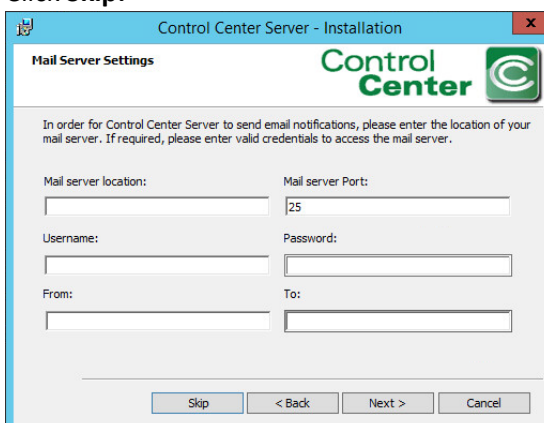
Control Center Server is going to use the following ports. If needed, you can change the port numbers below.

Web service port number:

Web application port number:

< Back Next > Cancel

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



Control Center Server - Installation

Mail Server Settings

In order for Control Center Server to send email notifications, please enter the location of your mail server. If required, please enter valid credentials to access the mail server.

Mail server location: Mail server Port:

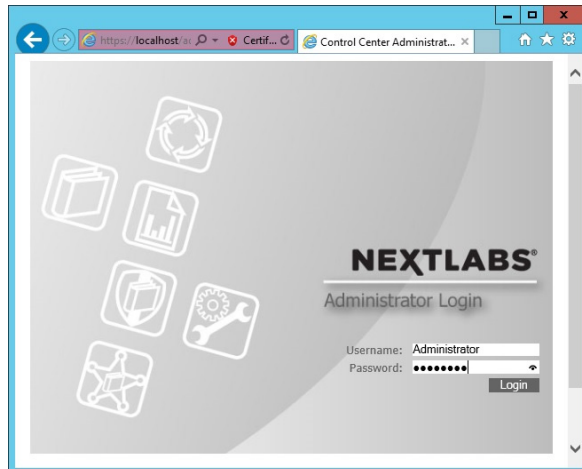
Username: Password:

From: To:

Skip < Back Next > Cancel

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

- 1128 a. Enter the Administrator Username and Password to log in.

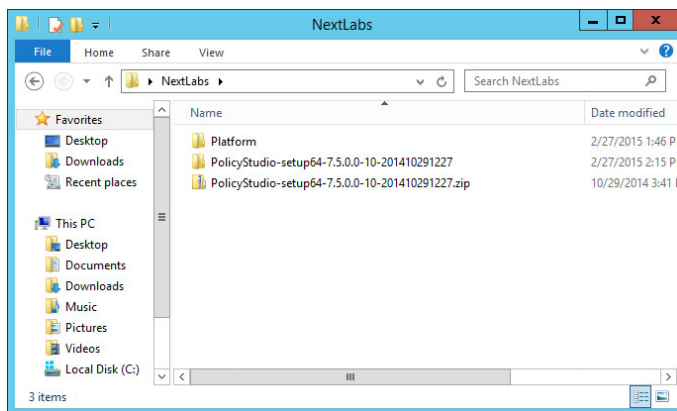


- 1129
1130 29. Once logged in to the Control Center Administrator web application in your browser, you can
1131 verify that the NextLabs Control Center is installed and configured correctly on the SQL Server.

1132 Policy Studio 7.7

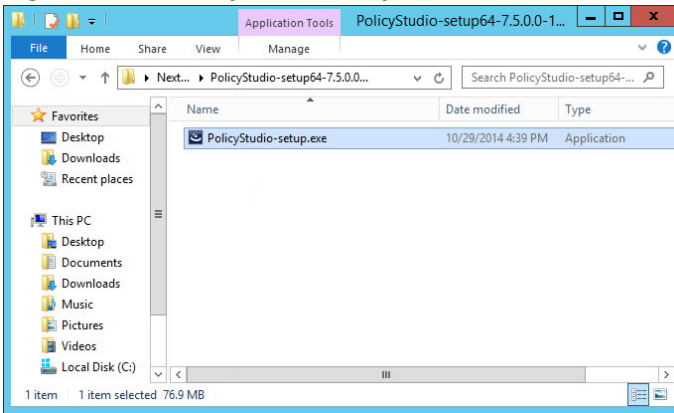
1133 Complete the standard Policy Studio installation per NextLabs documentation available to customers
1134 using the following steps:

- 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.

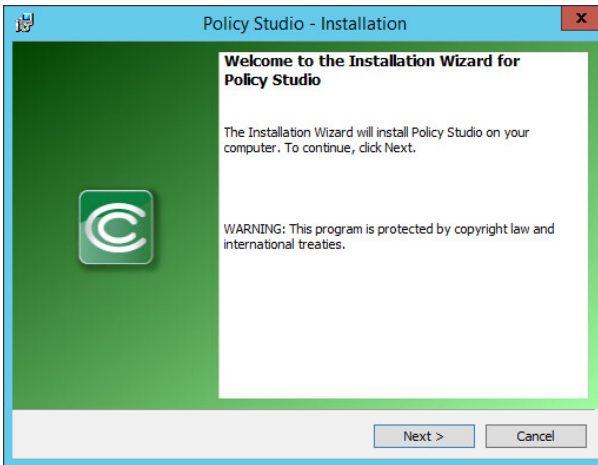


- 1139
1140 3. Double-click to open the **PolicyStudio-setup64-7.5.0.0-10-201410291227** folder.

- 1141 4. Right-click on **PolicyStudio-setup.exe** and select **Run as Administrator**.



- 1142 5. At the Welcome to the Installation Wizard for Policy Studio screen of the Policy Studio Installa-
1143 tion Window, click **Next**.
1144

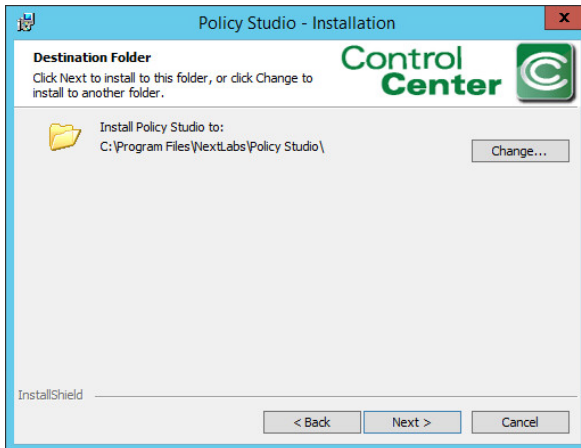


- 1145 6. At the License Agreement screen, select **I accept the terms in the license agreement**, and
1146 click **Next**.
1147



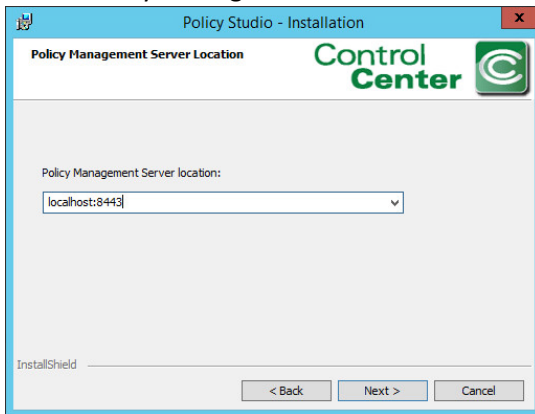
1148

- 1149 7. At the Destination Folder screen, click **Next**.



1150

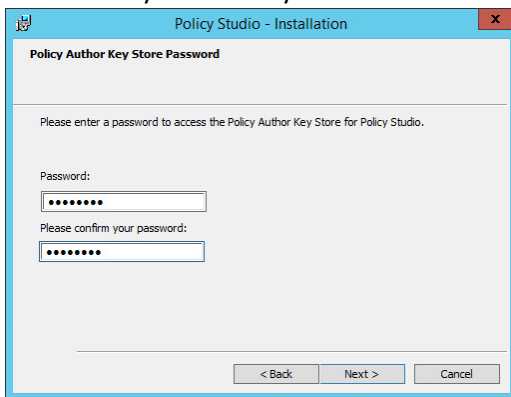
- 1151 8. At the Policy Management Server Location screen, enter the default location **localhost:8443**.



1152

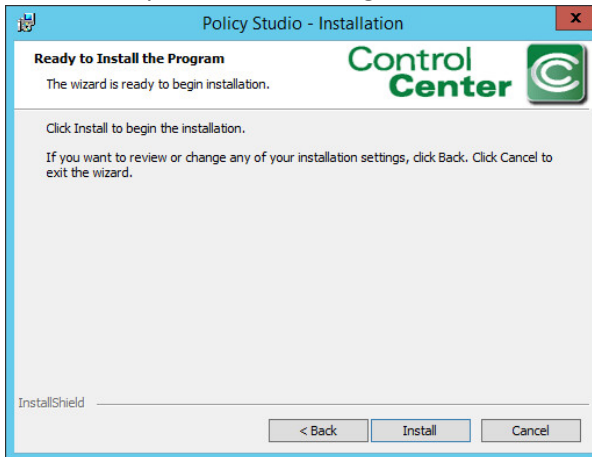
1153 Click **Next**.

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



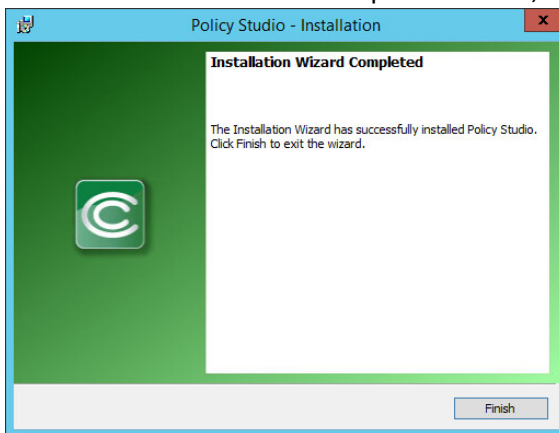
1155

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



1157

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



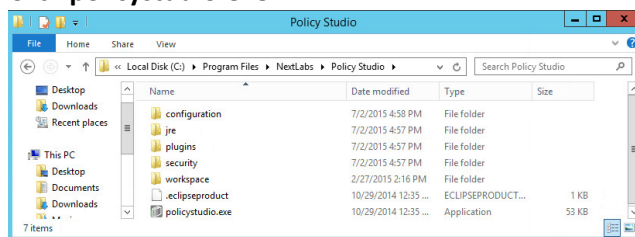
1159

1160 12. In Windows Explorer, find and open the **polycystudio.exe** application file.

1161

1162

- a. Navigate to the **C:/ drive>Program Files>NextLabs>Policy Studio**.
- b. Click **polycystudio.exe**.

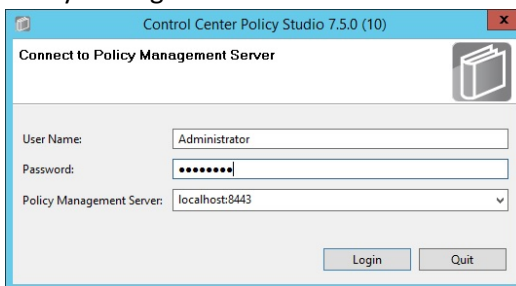


1163

1164

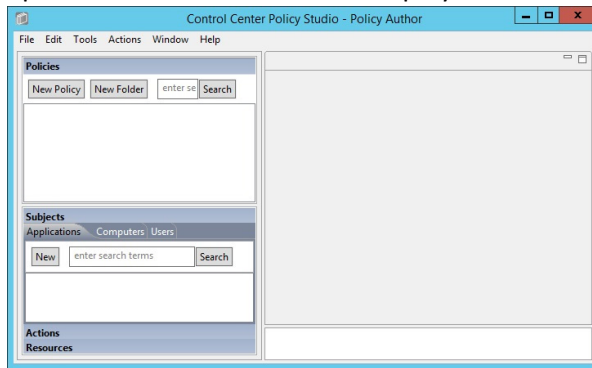
1165

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

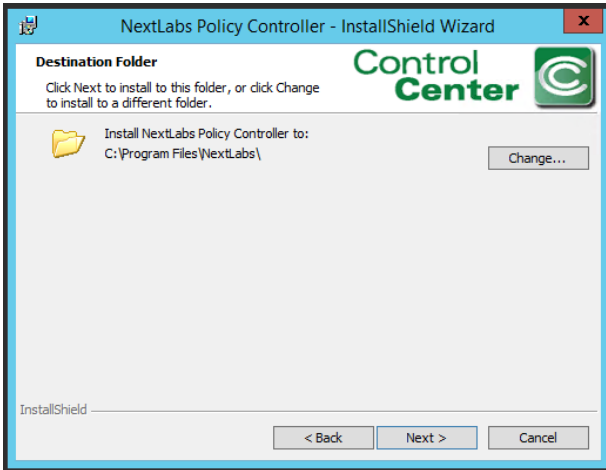
1171 The Policy Controller is installed on the SharePoint Server. To complete standard Policy Controller
 1172 installation per NextLabs documentation available to customers, use the following steps:

- 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**.



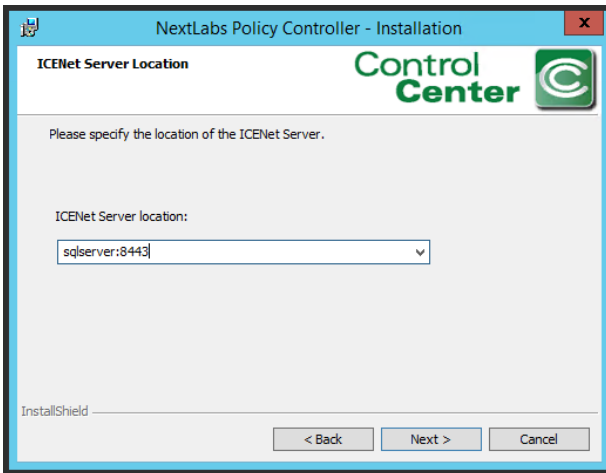
1182

1183 7. At the Destination Folder screen, click **Next**.



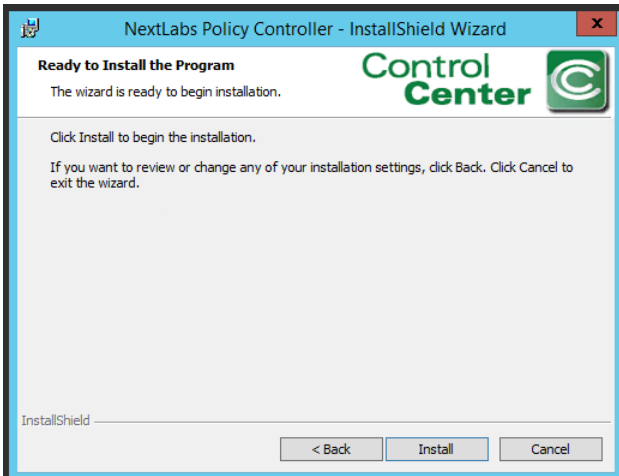
1184

1185 8. At the ICENet Server Location screen, enter the default ICENet Server Location: sqlserver:8443.
1186 Click **Next**.



1187

1188 9. At the Ready to Install the Program screen, click **Install**.



1189

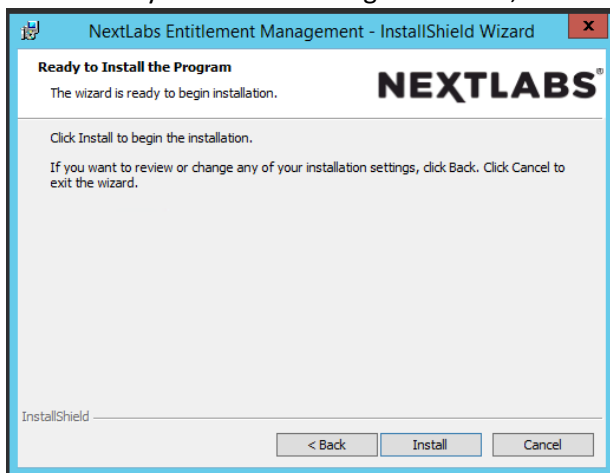
1190 10. At the InstallShield Wizard Completed screen, click **Finish**.

- 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.

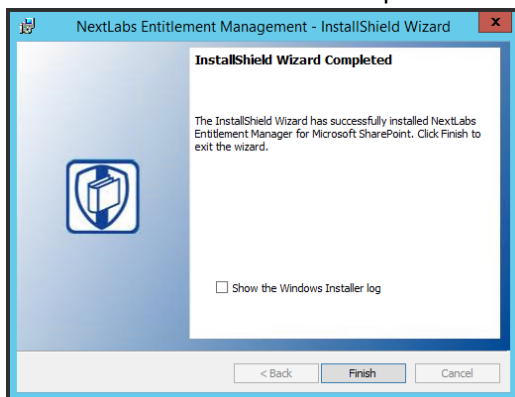
1193 **Entitlement Manager for Microsoft SharePoint 7.6**

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
1199 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-
1204 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**.



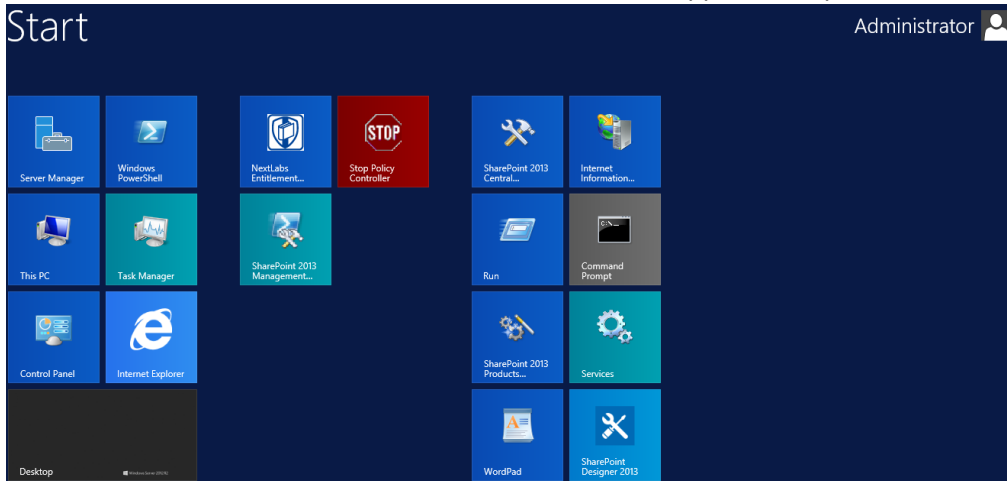
- 1207 8. At the InstallShield Wizard Completed screen, click **Finish**.



- 1209 9. After installing, the IIS server must be reset:
- 1210 a. Click the Windows icon and begin typing the word **PowerShell** and open the windows
1211 PowerShell application.
1212

1213 b. From within the Windows PowerShell window, type in this command and press **Enter** to
1214 reset Internet Information Services: **iisreset**.

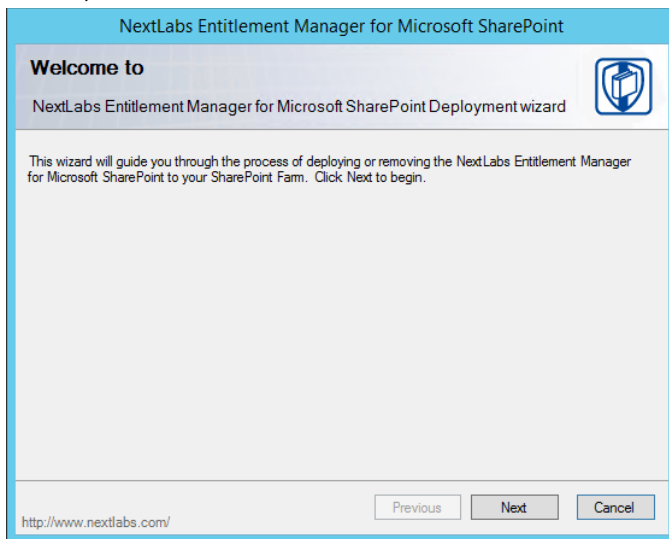
1215 10. On the SharePoint Server, click the **Start** icon to see the applications pinned to the **Start** menu.



1216
1217 11. Click the NextLabs Entitlement Manager for SharePoint Server Deployment icon.

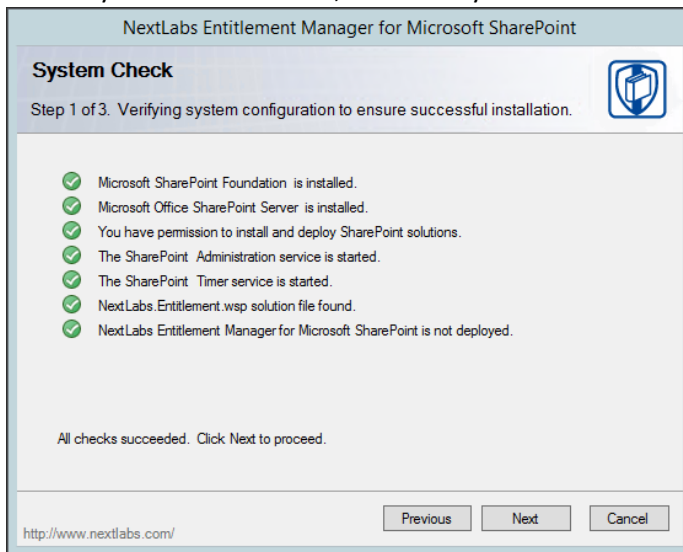
1218 This shortcut is automatically pinned during the initial installation. In case the shortcut is not created au-
1219 tomatically, the application can be opened from File Explorer at the **location: C:\Program**
1220 **Files\NextLabs\SharePoint Enforcer\bin\NextLabs.Entitlement.Wizard.exe**

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**.

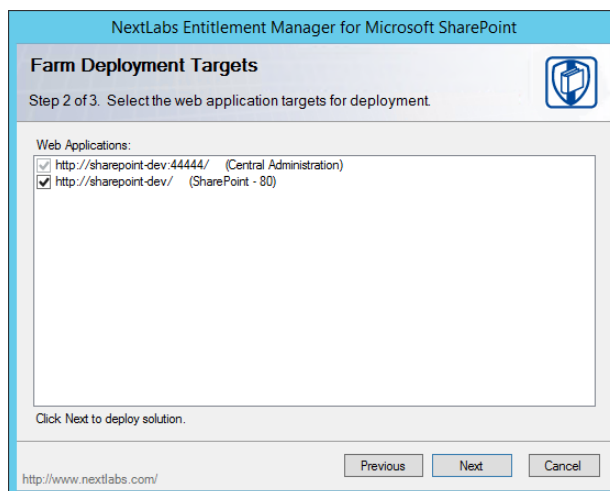


1225

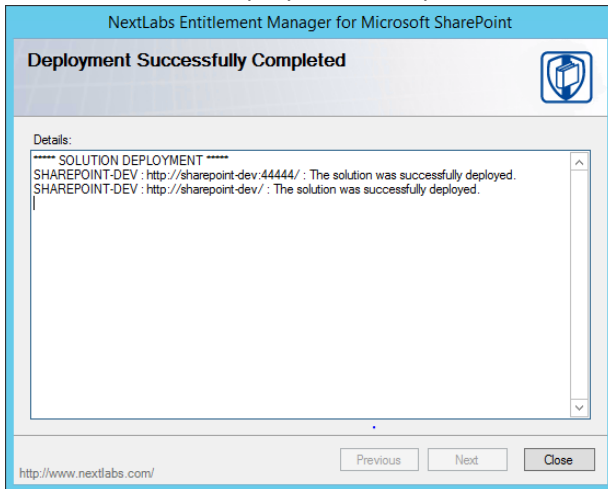
1226 14. At the Farm Deployment Targets screen, select the applicable web application on which to deploy.

1227 *Note:* If only one entry is listed, i.e., **http://sharepoint:44444/Central Administration**, no web appli-
1228 cations have been created.

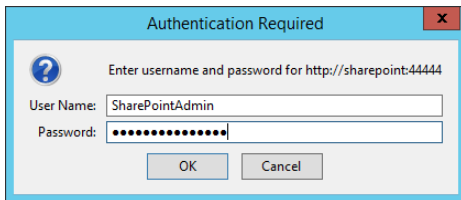
1229 15. At the Deploying Step 3 of 3 screen, click Next.



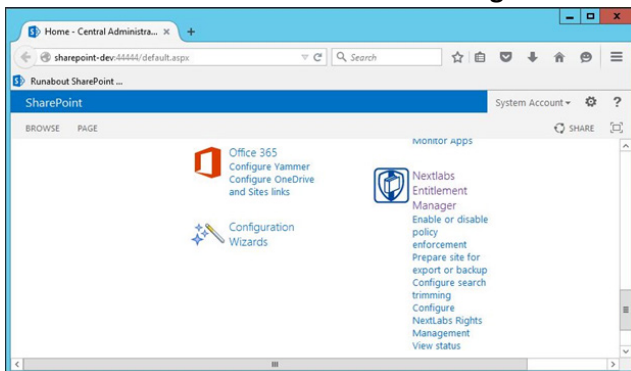
1230 16. At the Successful Deployment Completed screen, click **Close**.



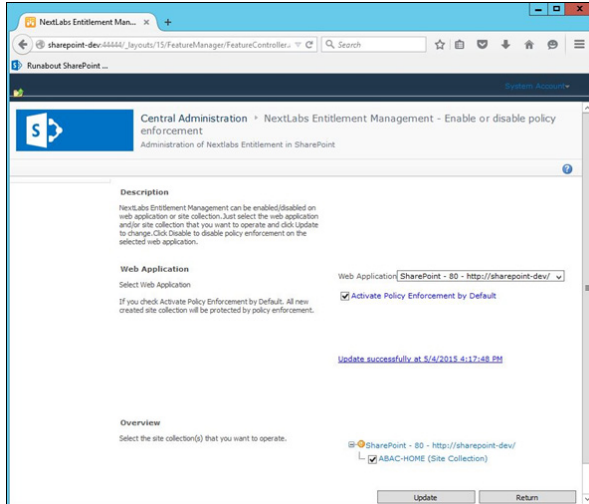
1231 17. Open a browser and navigate to the SharePoint Central Administration Portal. Log in with the
1232 SharePoint Administrator account.
1233



1234 18. Click on the **NextLabs Entitlement Manager** icon.
1235



1236 19. In the page that opens, scroll down to verify that the correct **Web Application** is chosen and the
1237 service is **Enabled**.
1238



1239

1240 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.

1244 2.5.1 How It's Used

1245 OpenLDAP stores user information and associated attributes for users who need access to Unix/Linux
 1246 based applications. Examples of such attributes are a user's userid, group, organizational unit, job title
 1247 and various other custom attributes. The OpenLDAP service listens and responds to requests from the
 1248 virtual directory service that acts as the enterprise policy information point and has the responsibility for
 1249 retrieving, organizing, and aggregating each user's attribute set under a single view.

1250 2.5.2 Virtual Machine Configuration

1251 The OpenLDAP virtual machine is configured as follows:

- 1252 ▪ Ubuntu Linux 16.04 LTS
- 1253 ▪ 1 CPU core
- 1254 ▪ 2GB of RAM
- 1255 ▪ 2 NICs
- 1256 ▪ 60GB of storage
- 1257 ▪ OpenLDAP server software

1258 Network Configuration (Interface 1)

1259 IPv4 Manual

1260 IPv6 Disabled

1261 IP Address: 192.168.19.11

1262 Netmask: 255.255.255.0

1263 Gateway: 192.168.19.1

DRAFT

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.

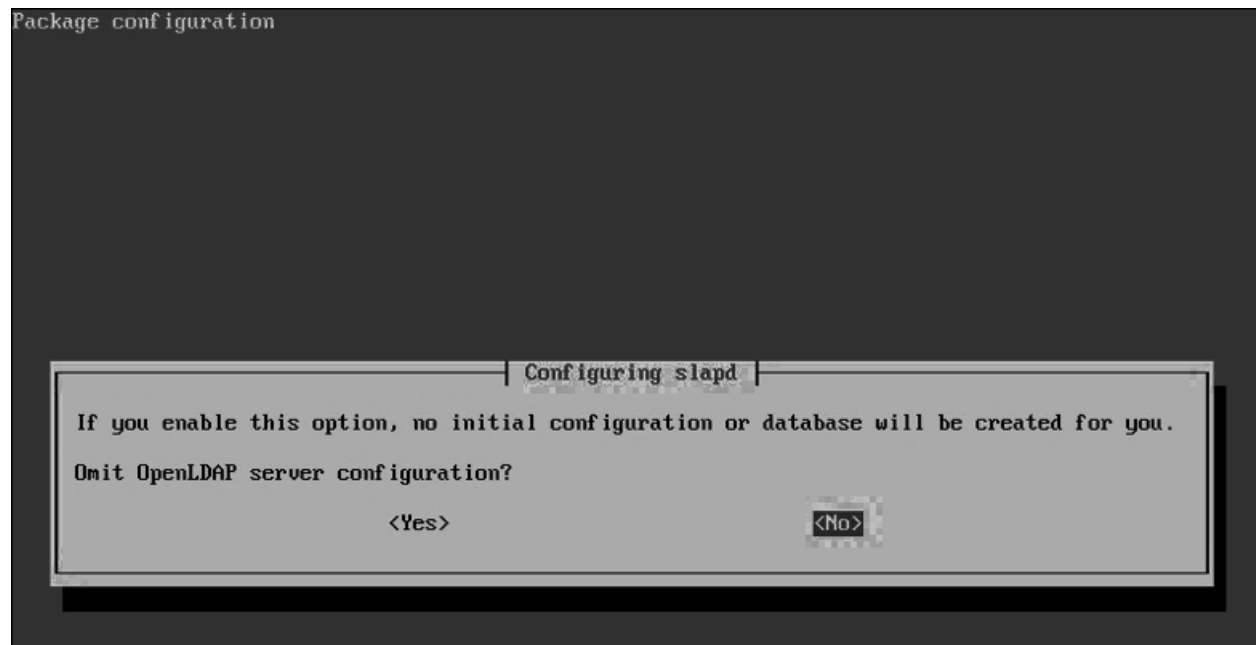
1276 `ufw allow 636/tcp to allow`
1277 `ufw allow 22/tcp to allow`
1278 `ufw default deny incoming`

1279 **2.5.4 Installation**

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

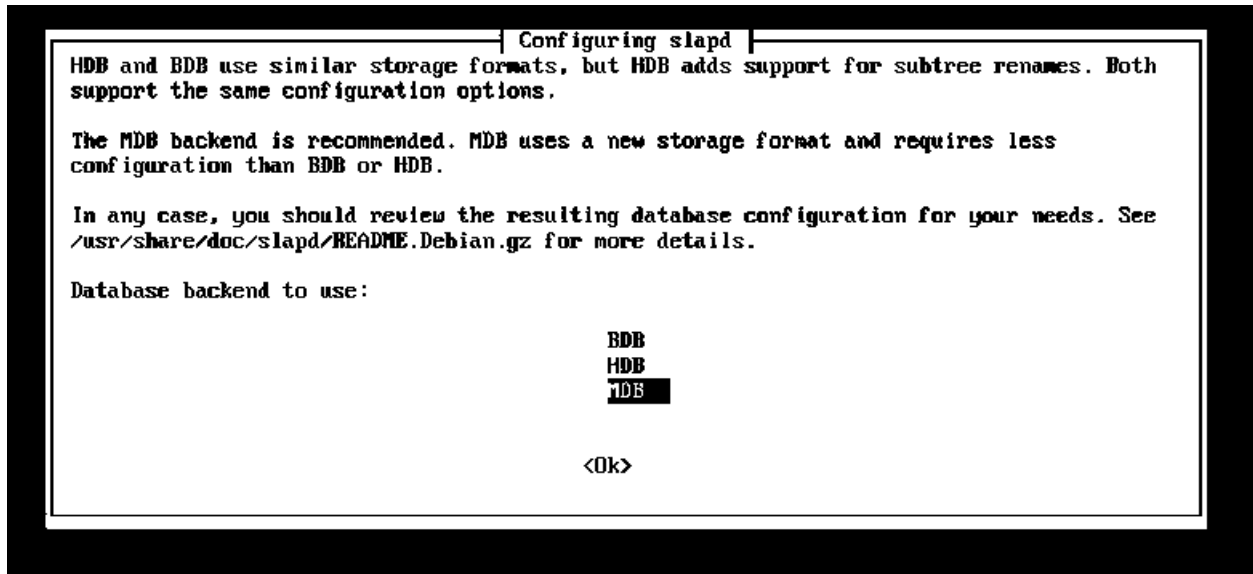
1280

Package configuration



1281

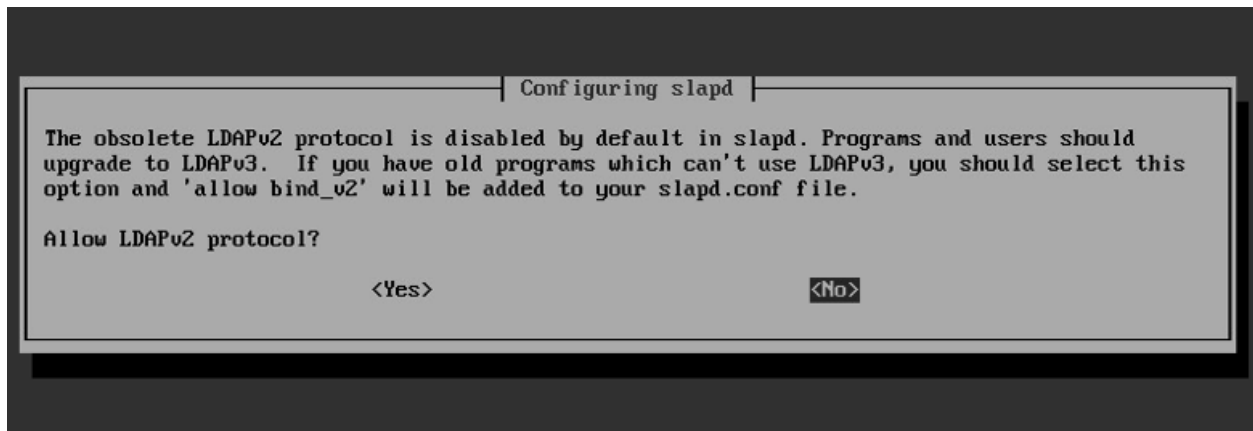
- 1282 1. Select **No** and press **Enter**.
- 1283 2. Enter the organizational Name on the following screen (for example, acmefinancial.com).
- 1284 3. Enter the administrator password for the BaseDN (BaseDN: acmefinancial.com).



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:

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

- 1298
 1299 4. Enter `ldapadd -Q -Y -EXTERNAL -H ldapi:/// -f create-cn-module.ldif` to add the cn
 1300 module.
 1301 5. Enter `touch logging.ldif`. The file contents should be as follows:

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

- 1302
 1303 6. Enter `chmod 775 /etc/ldap/logs`.
 1304 7. Enter `chmod 664 /etc/ldap/logs/auditlog.log`.
 1305 8. Enter `ldapadd -Q -Y -EXTERNAL -H ldapi:/// -f logging.ldif`.
 1306 9. Changes to user records should now appear in `/etc/ldap/logs/auditlog.log`.
 1307

1308 2.5.6 STARTTLS and LDAPS Configuration

- 1309 1. On the OpenLDAP server, create an ssl directory `/etc/ldap/ssl`. Enter `mkdir /etc/ldap/ssl`.
 1310 2. Move the certificates created for the OpenLDAP server from the Certificate of Authority to the
 1311 ssl subdirectory:
 1312 a. `scp openldap_cert.pem user1@openldap.acmefinancial.com:/ldap/ssl`
 1313 b. `scp openldap_privatekey.pem user1@openldap.acmefinancial.com:/ldap/ssl`
 1314 c. `scp acmefinancial.com-CA.pem user1@openldap.acmefinancial.com:/ldap/ssl`
 1315 3. Install the CA certificate so that local applications can use the certificate when necessary:
 1316 a. `cp acmefinancial.com-CA.pem /usr/share/ca-certificates/acmefinan-`
 1317 `cial.com-CA.crt`
 1318 b. Add `acmefinancial.com-CA.crt` to the end of the `/etc/ca-certificates.conf` file.
 1319 c. Enter `sudo update-ca-certificates`.
 1320 4. Create a certificate information file called `certinfo.ldif` in `/etc/ldap/ssl` with the following con-
 1321 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
1323 5. Set permissions and ownership on the certificate files so that the openLDAP user can read the
1324 key file:

- 1325 a. `sudo adduser openldap ssl-cert`
1326 b. `chgrp ssl-cert /etc/ldap/ssl/openldap_privatekey.pem`
1327 c. `chmod g+r /etc/ldap/ssl/openldap_privatekey.pem`
1328 d. `chmod o-r /etc/ssl/ldap/openldap_privatekey.pem`
1329 e. `chown root:ssl-cert /etc/ldap/ssl/openldap_privatekey.pem`
1330 f. `chown root:ssl-cert /etc/ldap/ssl/openldap_cert.pem`
1331 g. `chmod root:ssl-cert /etc/ldap/ssl`

- 1332 6. Reconfigure slapd by running the following command
1333 a. `ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/ldap/ssl/certinfo.ldif`
1334 b. 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:

1337

```

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

```

1338

- 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 loca-
1346 tion of your CA certificate.

```

# TLS certificates (needed for GnuTLS)
#TLS_CACERT      /etc/ssl/certs/ca-certificates.crt
1347 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
1374 import datetime
1375 start_index = 0
1376 end_index = 0
1377 timestamp = 123456789 #var to store datetime object; values are placeholders
1378 localtime = "12345" #string var to store local time; values are placeholders
1379 filename = "/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
1382 with 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

```

DRAFT

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](#).

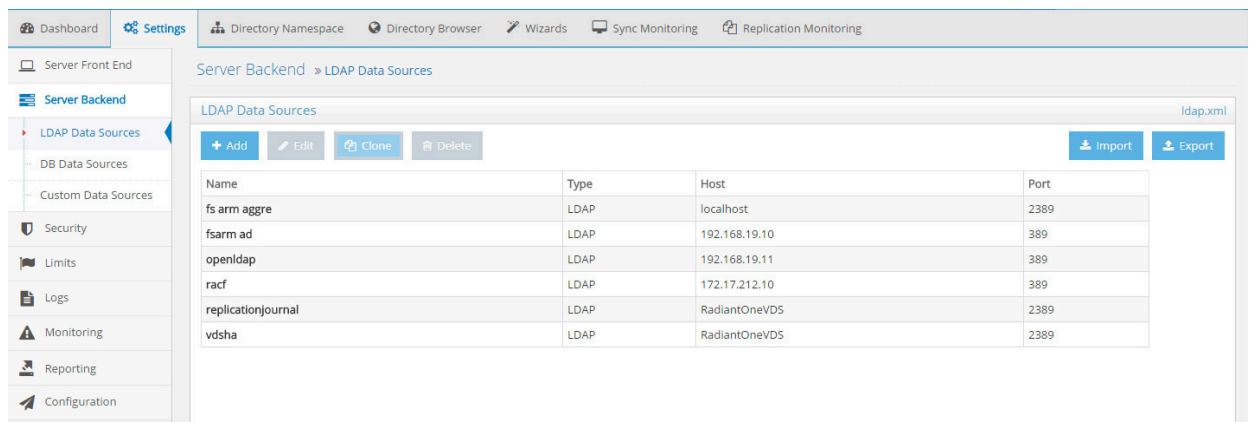
1457 **2.6.4 Configuring VD**

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**
1466 **Sources,**
- 1467 2. Click **Add**.



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**.

The screenshot shows the 'Edit LDAP Data Source' configuration page. The 'Data Source Name' is 'fsarm ad', 'Data Source Type' is 'AD2008', and 'Status' is 'Active'. The 'Host Name' is '192.168.19.10', 'Bind DN' is 'Administrator@acmefinancial.com', and 'Base DN' is 'DC=AcmeFinancial,DC=com'. The 'Port' is '389' with 'SSL' checked. The 'Bind Password' is masked with dots. There are checkboxes for 'Use Kerberos profile' (set to 'vds_krb5'), 'Disable Referral Chasing' (checked), 'Paged Results Control, page size' (set to 600), and 'Verify SSL Certificate Hostname' (unchecked). A 'Test Connection' button is visible. Below the main form are sections for 'Failover LDAP Servers' and 'Advanced' settings.

1471 **Note:** Be sure to select **Disable Referral Chasing** for AD.
 1472

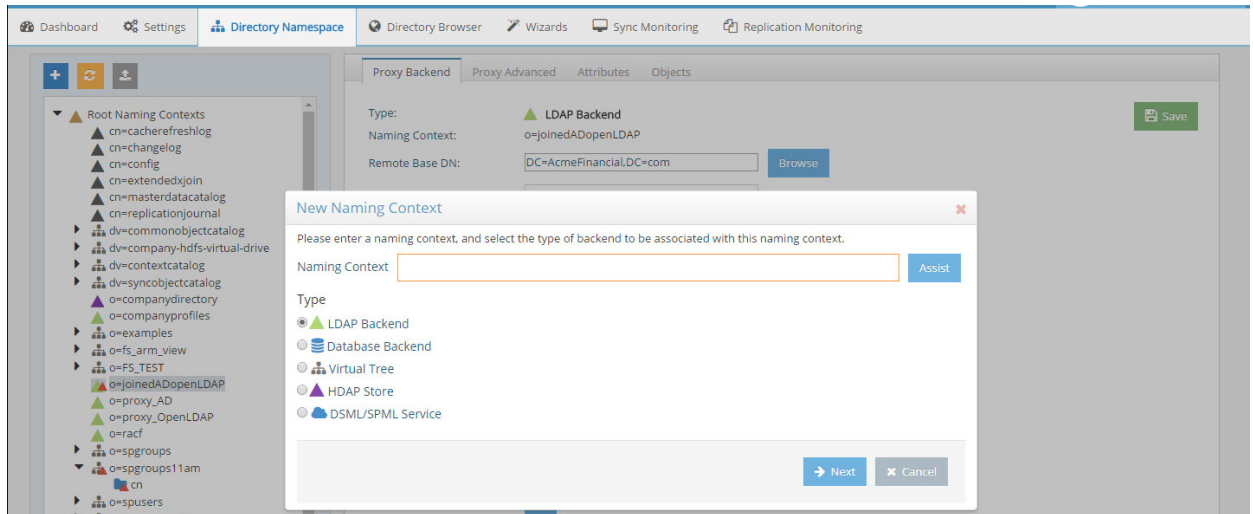
- 1473 4. Repeat Steps 2 and 3 for the OpenLDAP and RACF directories. Use LDAP as the data source type.
 1474 Details for each are shown in the following screenshots:

The screenshot shows the 'Edit LDAP Data Source' configuration page for an OpenLDAP data source. The 'Data Source Name' is 'openldap', 'Data Source Type' is 'LDAP', and 'Status' is 'Active'. The 'Host Name' is '192.168.19.11', 'Bind DN' is 'cn=admin,dc=acmefinancial,dc=com', and 'Base DN' is 'dc=acmefinancial,dc=com'. The 'Port' is '389' with 'SSL' checked. The 'Bind Password' is masked with dots. There are checkboxes for 'Use Kerberos profile' (set to 'vds_krb5'), 'Disable Referral Chasing' (unchecked), 'Paged Results Control, page size' (set to 0), and 'Verify SSL Certificate Hostname' (unchecked). A 'Test Connection' button is visible. Below the main form are sections for 'Failover LDAP Servers' and 'Advanced' settings.

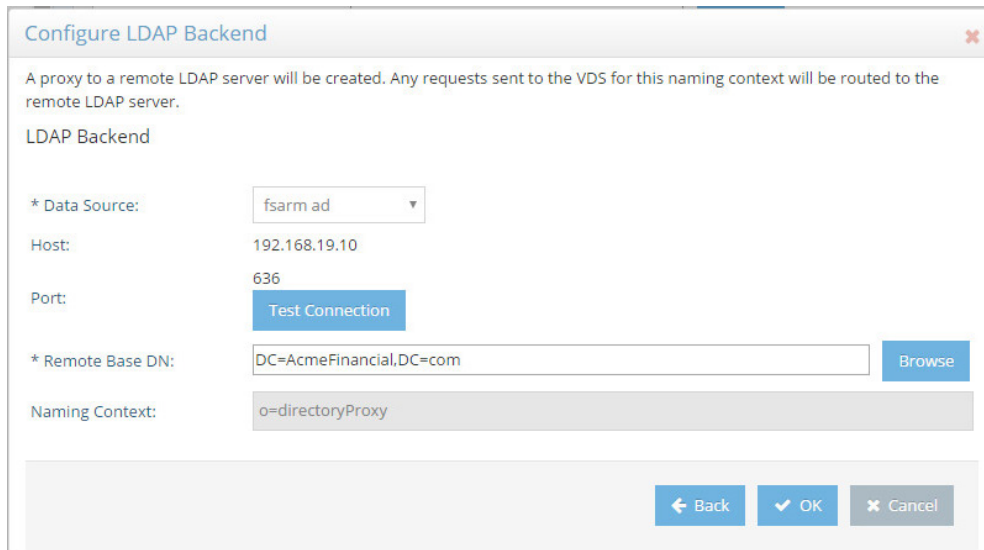
The screenshot shows the 'Edit LDAP Data Source' configuration page for a RACF data source. The 'Data Source Name' is 'racf', 'Data Source Type' is 'LDAP', and 'Status' is 'Active'. The 'Host Name' is '172.17.212.10', 'Bind DN' is 'racfid=TSNI00,profiletype=user,SYSPLEX=SYSPLEX1', and 'Base DN' is 'SYSPLEX=SYSPLEX1'. The 'Port' is '389' with 'SSL' checked. The 'Bind Password' is masked with dots. There are checkboxes for 'Use Kerberos profile' (set to 'vds_krb5'), 'Disable Referral Chasing' (unchecked), 'Paged Results Control, page size' (set to 0), and 'Verify SSL Certificate Hostname' (unchecked). A 'Test Connection' button is visible. Below the main form are sections for 'Failover LDAP Servers' and 'Advanced' settings.

- 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**.

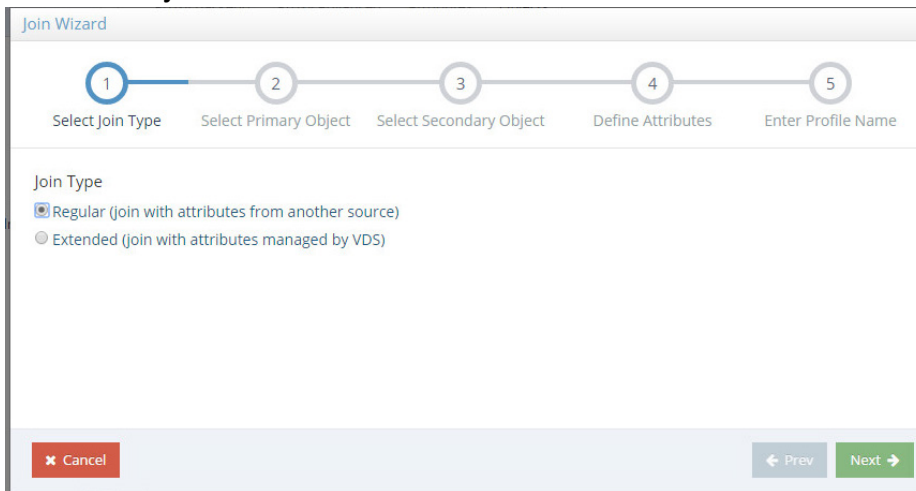


- 1482 3. Select the name of the AD backend created earlier as the **Data Source**. Select the **Remote Base**
- 1483 **DN** of the domain. Select **OK**.
- 1484

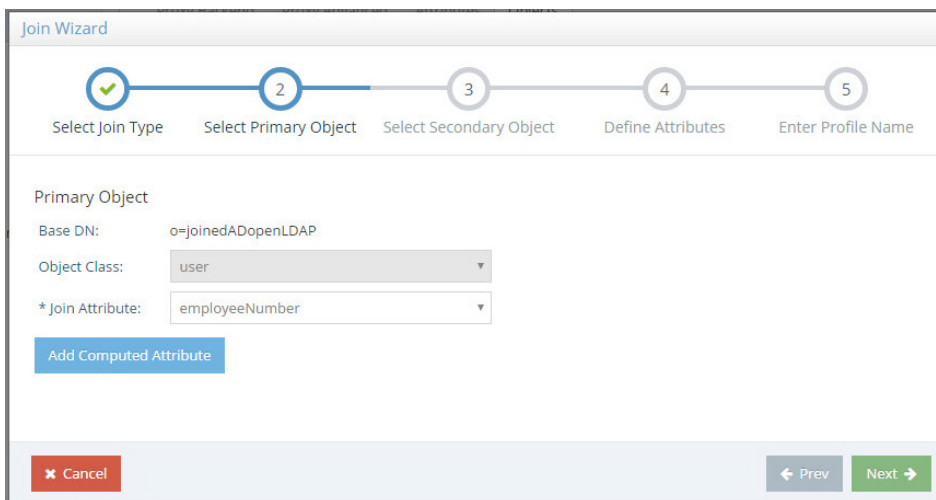


- 1485 4. When the LDAP proxy is created, select the root naming context created in the left window
- 1486 pane.
- 1487

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



- 1489 6. Choose **Regular**. Click **Next**.
 1490
 1491 7. Select **employeeNumber** as the Join Attribute. Click **Next**. *Note:* The employee number must be
 1492 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

Progress: 1 (✓) — 2 (✓) — 3 — 4 — 5

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 ← Prev Next →

1497

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

Join Wizard

Progress: 1 (✓) — 2 (✓) — 3 (✓) — 4 — 5

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

Return attributes

All attributes

Attributes listed below:

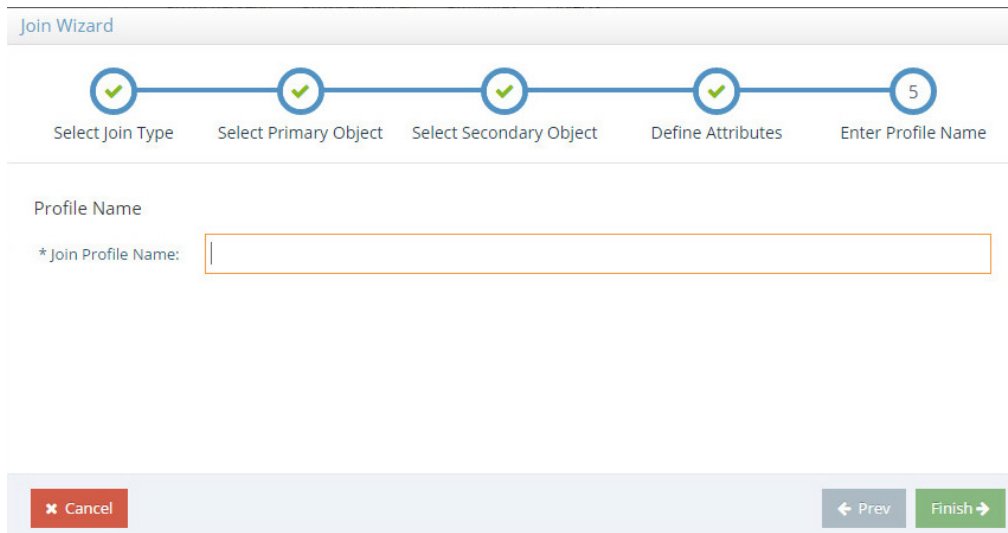
+ Add ✖ Remove

Actual Name	Virtual Name
audio	
businessCategory	
carLicense	
cn	
departmentNumber	

✖ Cancel ← Prev Next →

1499

1500 10. Name the Join Profile. Click **Finish**.

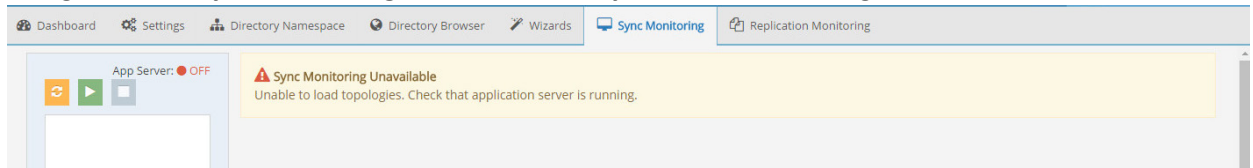


1501
1502 11. Repeat Steps 5–10 to join the RACF directory using the appropriate RACF objectClass and Base
1503 DN.

1504 2.6.5 Configure Logging

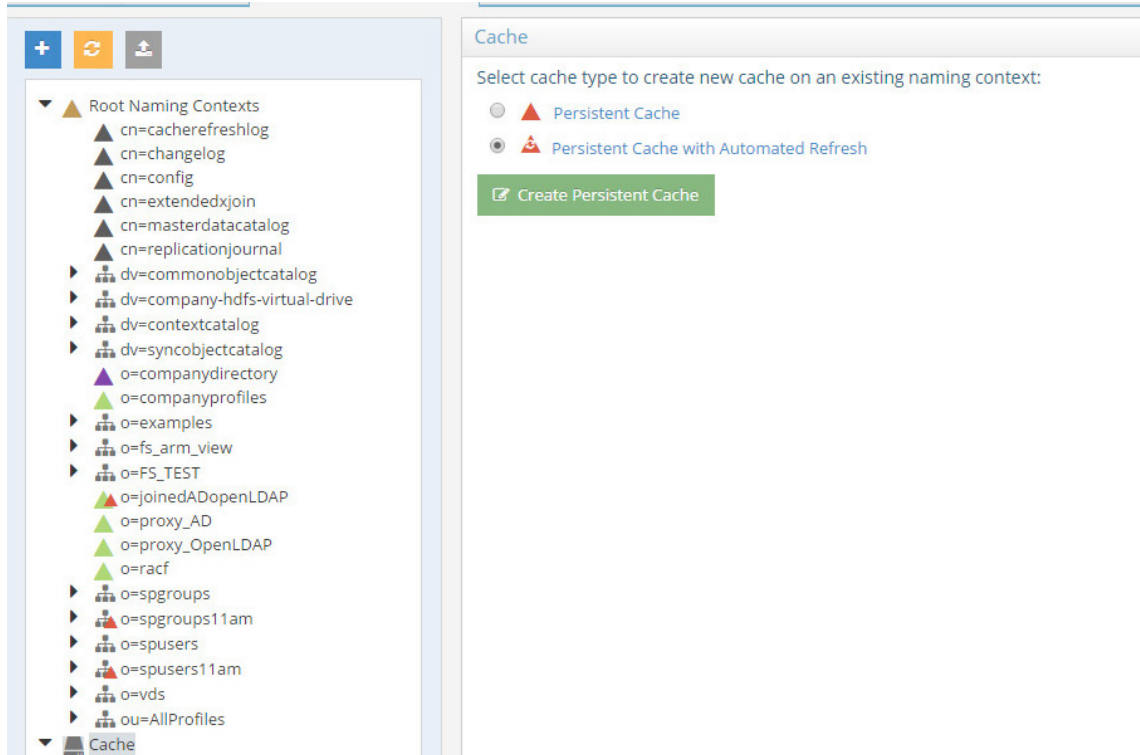
1505 To log changes to each directory object, you must create a cache for the proxy view created in the
1506 previous section. To create the cache and log changes made to the backend directories, complete the
1507 following steps:

1508 1. Navigate to the **Sync Monitoring** tab. Press the **Play** button to start the glassfish server.

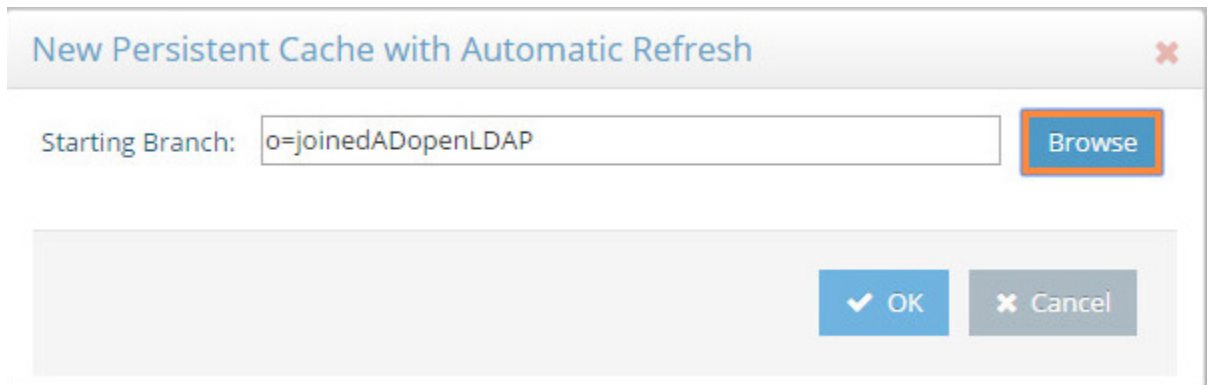


1509

- 1510 2. In the **Directory Namespace** tab, highlight **Cache** in the left window pane. Select **Persistent**
1511 **Cache with Automated Refresh**. Click **Create Persistent Cache**.

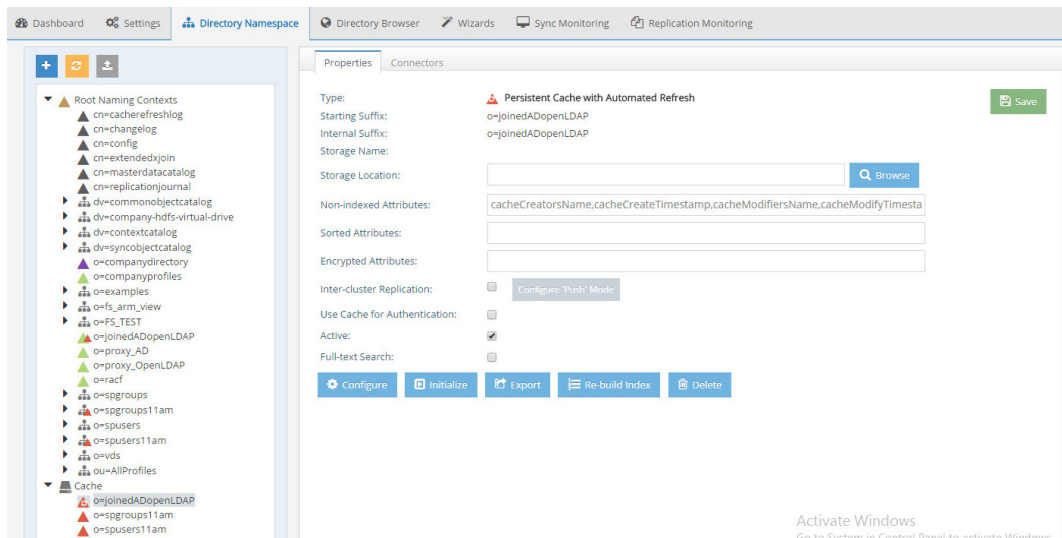


- 1512 3. Browse and select the LDAP proxy created in the previous section. Select **OK**. The VD creates the
1513 cache.
1514

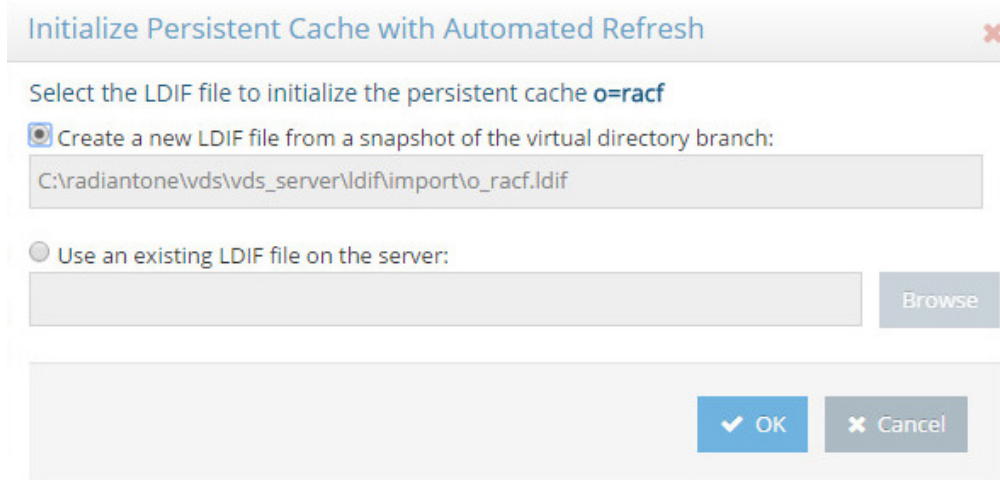


1515

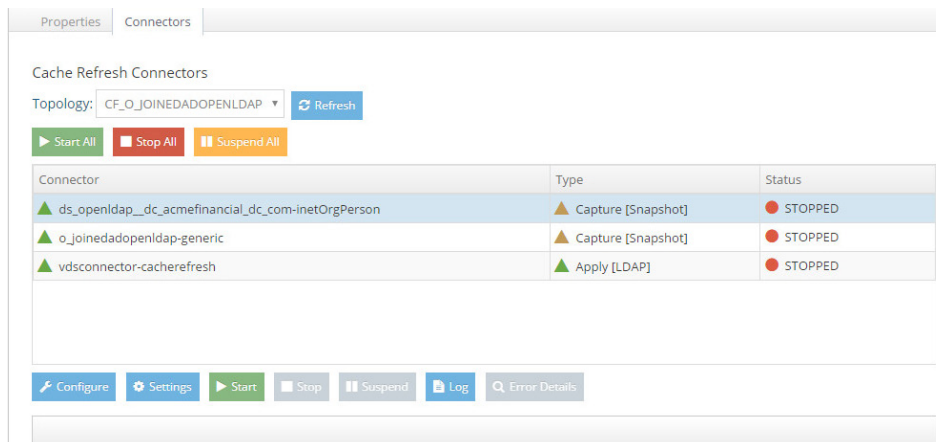
- 1516 4. Select the created cache from the lower left window. Click **Initialize** to make the cache active.



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

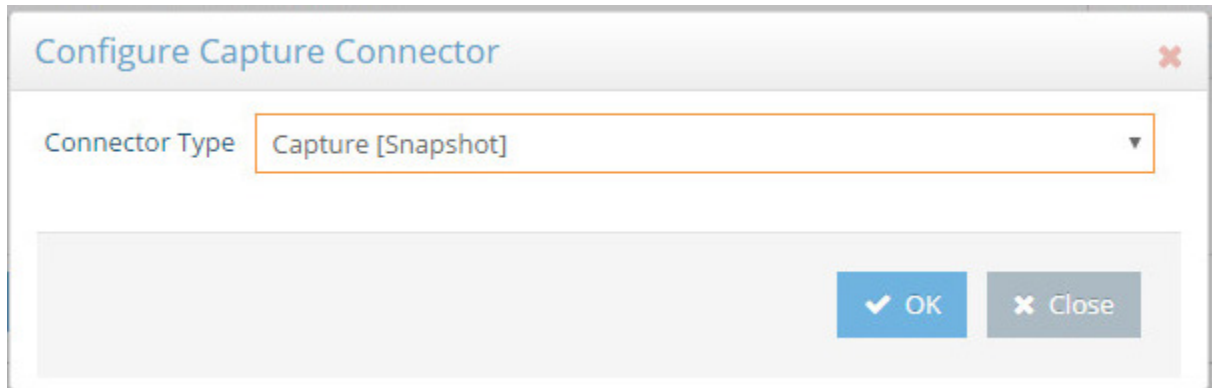


- 1520 6. Once complete, **Save** the settings.
 1521
 1522 7. Select the **Connectors** tab.

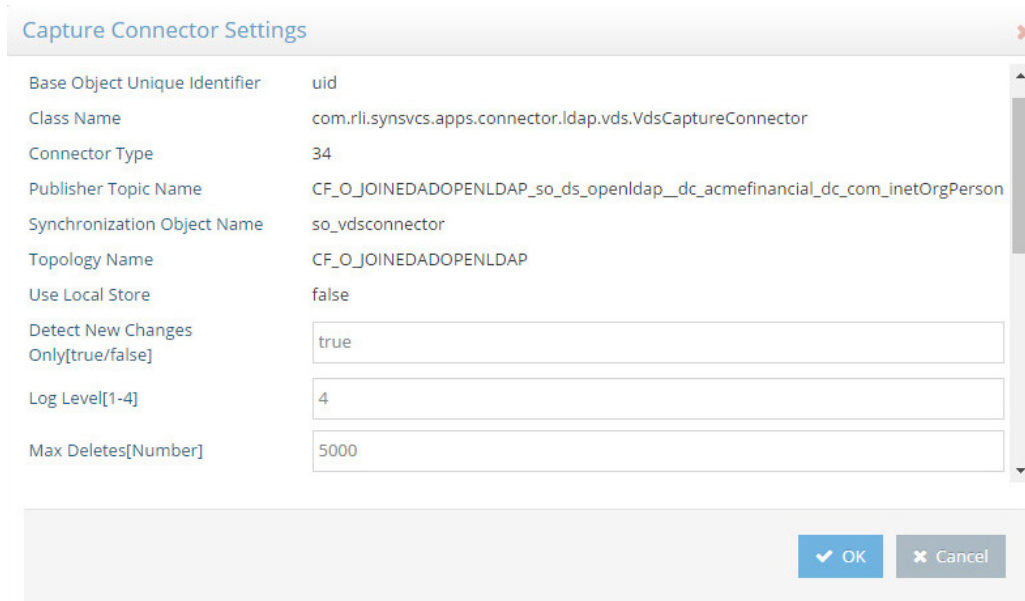


1523

- 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."

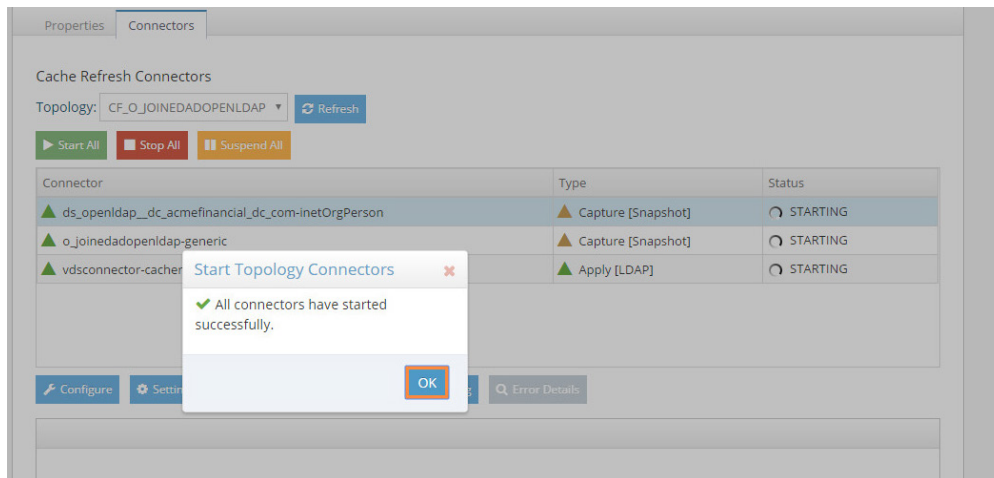


- 1528 9. Back at the **Connectors** tab, highlight the first connector. Select **Settings**. Change the log level to
1529 the number 4. Click **OK**. Repeat this step for each connector except the "vdsconnector-
1530 cacherefresh."
1531

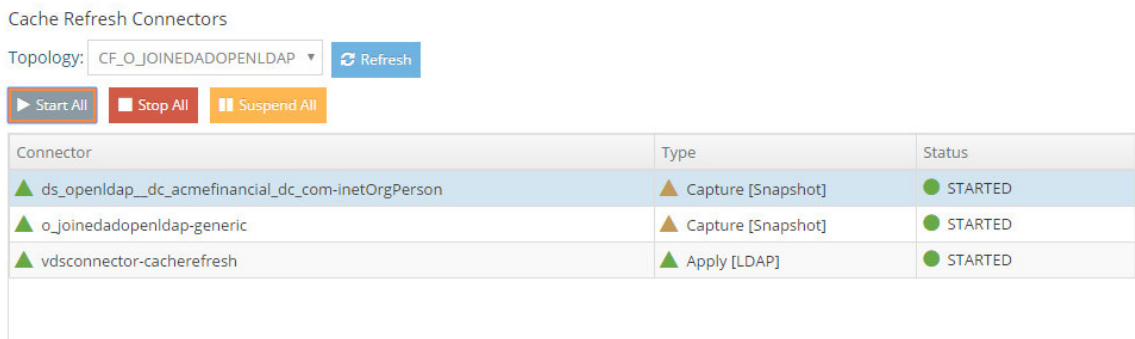


1532

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



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



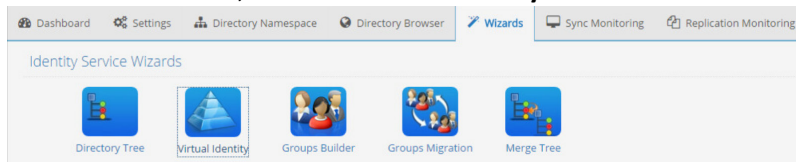
1537

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**.

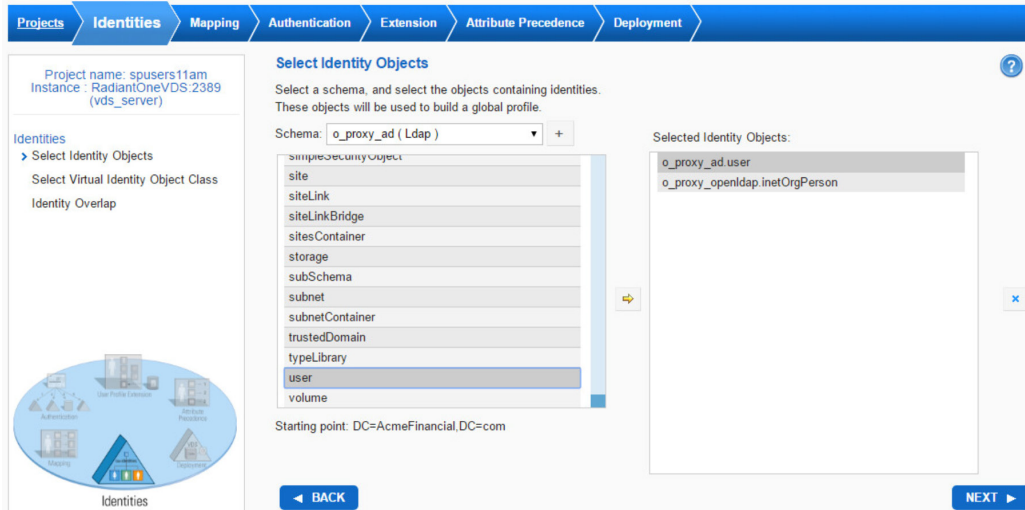


- 1546 2. Click **Next**.
 1547 3. Click **New** and enter a project name (e.g., spusers) and click **Next**.
 1548 4. If you do not already have the schemas extracted from the data sources (or even data sources
 1549 defined), use the **+** button to do so. The schema objects selected must be the ones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

1553
1554
1555
1556
1557
1558

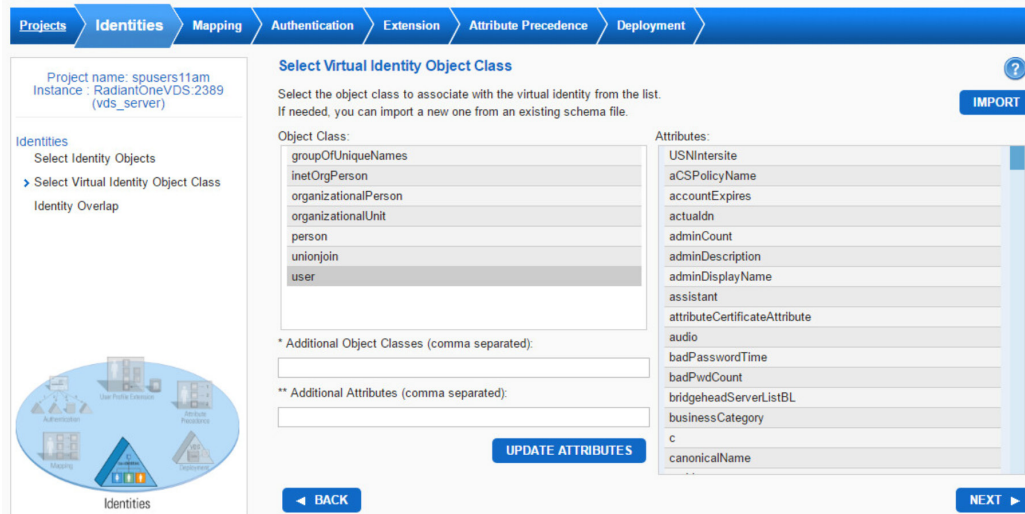
Guide.

- 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.”
- Create the Selected identity objects shown below with the user schema from the AD backend and the inetOrgPerson from the openLDAP backend.



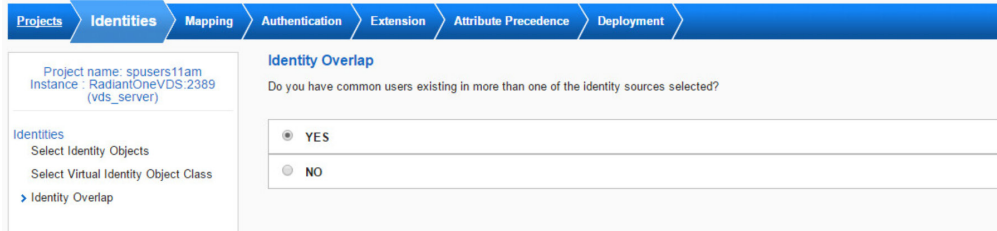
1559
1560
1561
1562
1563
1564

- Click **Next**.
- 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.



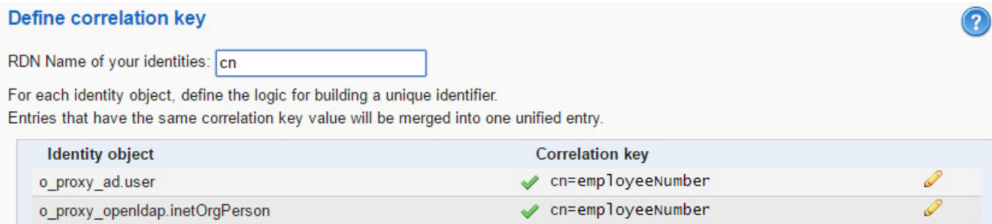
1565
1566
1567

- Click **Next**.
- Select **Yes**. Click **Next**.




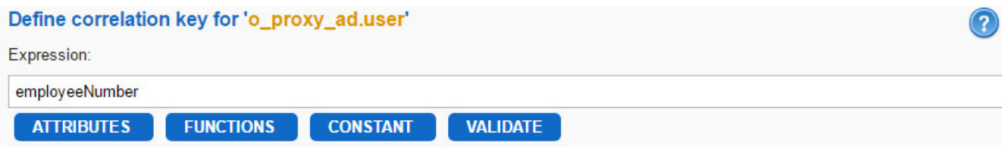
1568
1569

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



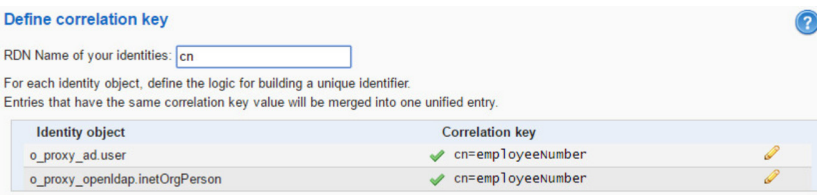
1570
1571
1572

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



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**.



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

Attribute mappings from 'o_proxy_ad.user' to '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

← 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_openldap.inetOrgPerson

Attribute mappings from 'o_proxy_openldap.inetOrgPerson' to 'user'

Source attribute	map to	Virtual identity attribute
		dynamicLDAPServer
		employeeID
employeeNumber		employeeNumber
		employeeType
		extensionName
		fRSMemberReferenceBL
		fSMORoleOwner
		facsimileTelephoneNumber
		flags
		fromEntry
		frsComputerReferenceBL
		generationQualifier
givenName		givenName
		groupMembershipSAM

← 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

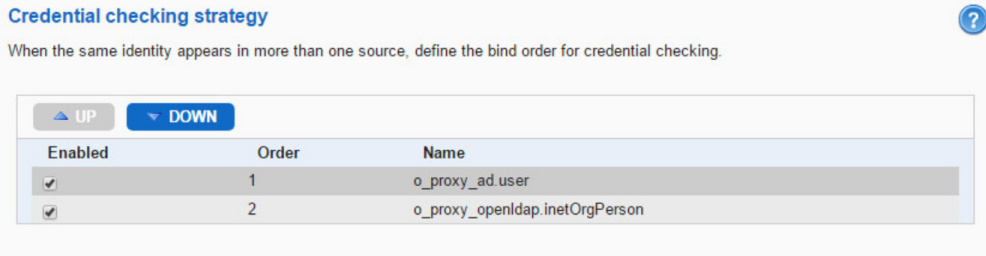
Select how you would like to identify the users.

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

- uSNCLastObjRemoved
- uSNLastObjRem
- uSNSource
- uid
- unicodePwd
- url
- userAccountControl

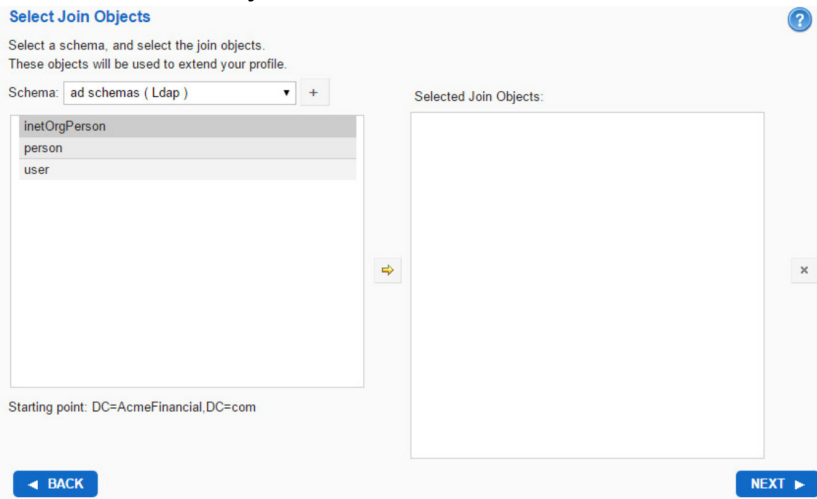
1585
1586
1587

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



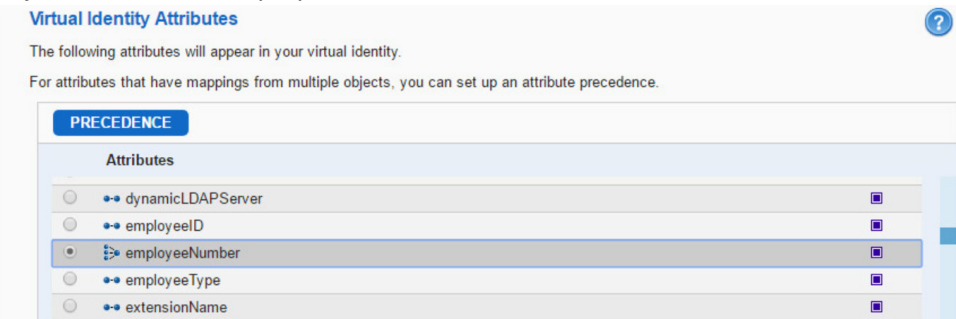
1588
1589

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



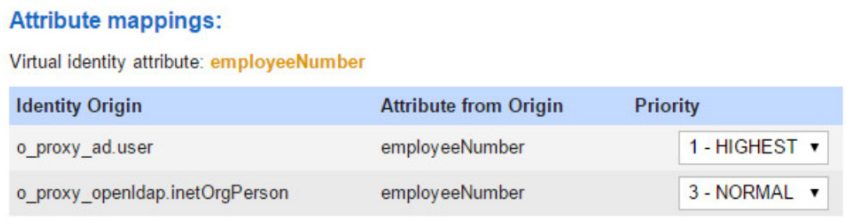
1590
1591
1592

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



1593
1594

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



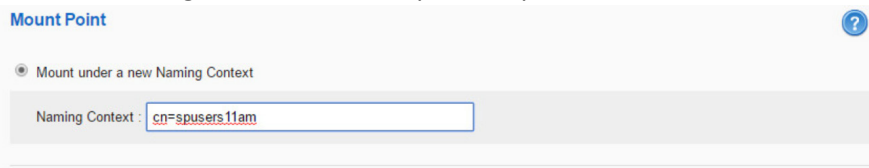
Warning: The runtime processes the priority in 2 steps: the identities origins (union) then the extension origins (joins). The highest priority set on the union is going to be processed and compared at runtime with the priority set on each join.



1595
1596

21. Click **Next**.

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



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

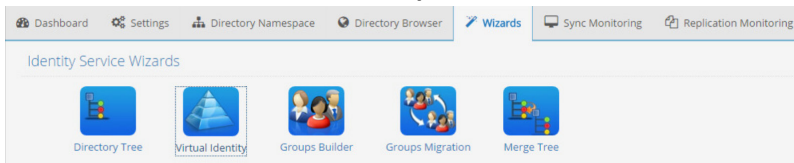


1600 24. Define the refresh interval. Click **Next**.

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

1603 Follow these steps to configure the groups for SharePoint:

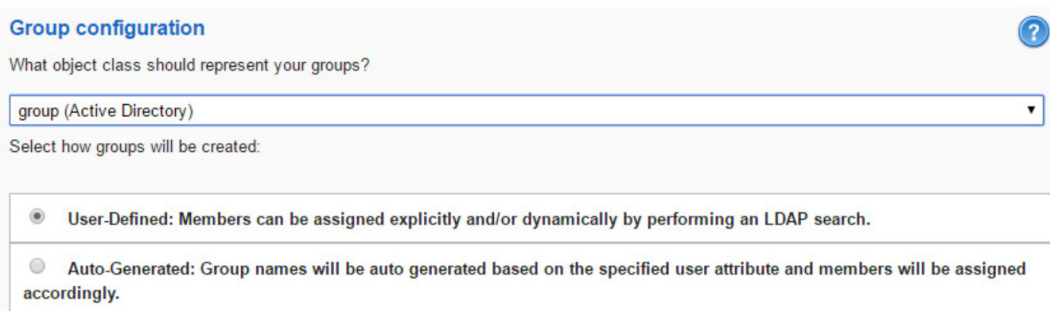
1604 1. On the **Wizards** tab, click the **Groups Builder Wizard**.



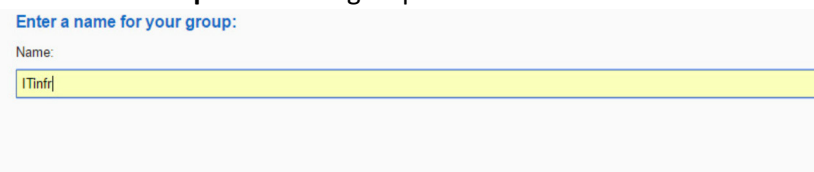
1605 2. Click **Next**.

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*.

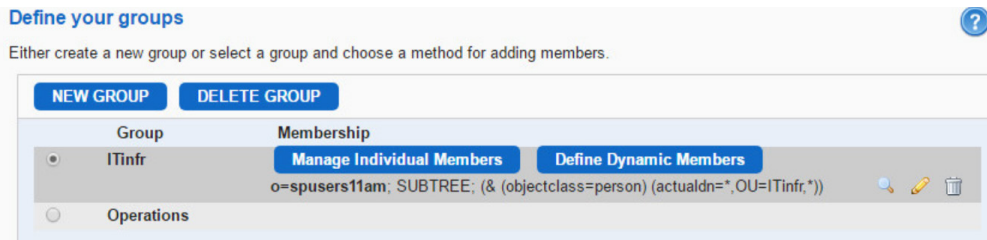


1611 5. Select **New Group**. Name the group ITinfr. Click **Next**.



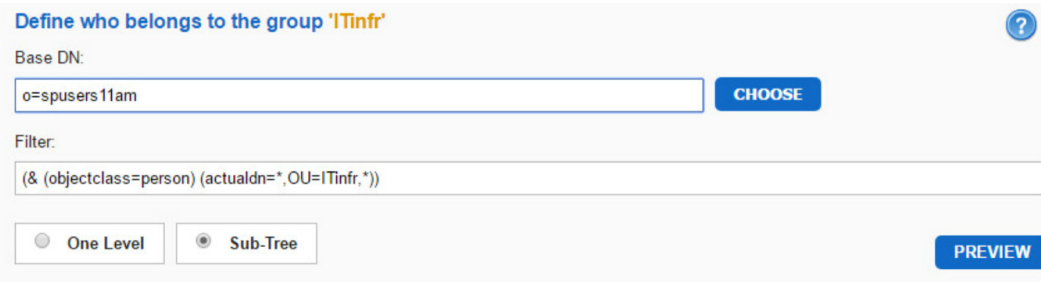
1613 6. Repeat Step 5. Name the group Operations.

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



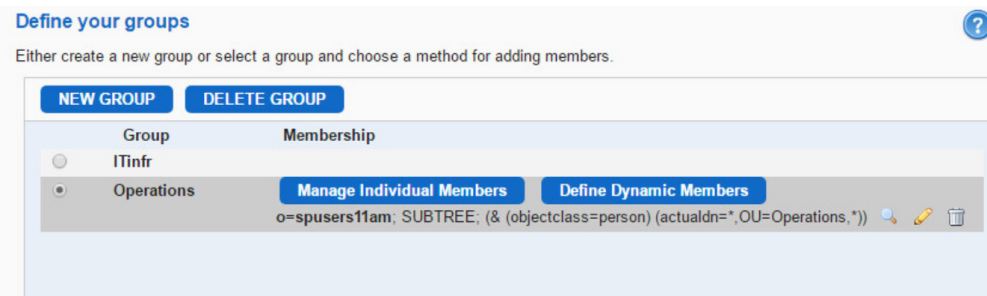
1616
1617
1618
1619

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



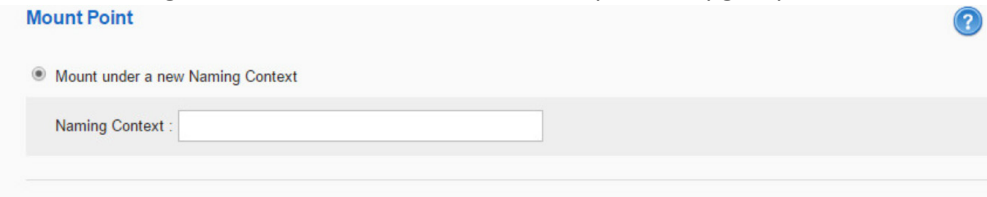
1620
1621
1622
1623

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



1624
1625

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



1626
1627

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



1628
1629
1630
1631

- Define the refresh interval. Click **Next**.
- 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 yyy"
1656     #Overwrite the contents of prevtime-file.txt with the current date
1657     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > 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     }
```

DRAFT

```
1673     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
1674     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\Radiant\prevtime-
1675     file.txt
1676     $HostVar = hostname
1677     $Status = 'offline'
1678     Add-Content C:\scripts\Radiant\Radiant-Status-Output.csv
1679     $CurrentTime','$HostVar','$Status','$PrevTime
1680     }
1681 2.6.9 Script: VanguardOnlineStatus.ps1
1682 #Script checks if the RACF mainframe is online and outputs status messages to file
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 yyy"
1698     #Overwrite the contents of prevtime-file.txt with the current date
1699     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > 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 yyy"
1714     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > 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 }

```

1721 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.

1732 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.

1735 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.

1738 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.

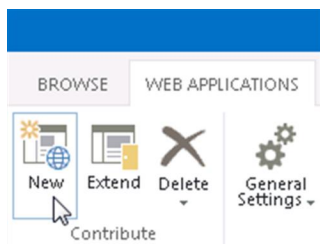
1755 2.7.4 Installing SharePoint 2013

- 1756 1. Installing SQL Server 2012: On the server where SharePoint 2013 is going to be installed, follow the
1757 steps from this link to install SQL Server 2012: [https://technet.microsoft.com/en-](https://technet.microsoft.com/en-us/library/ms143219(v=sql.110).aspx)
1758 [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,
1760 follow the steps from this link to install IIS 8.0: [http://www.iis.net/learn/get-started/whats-new-in-](http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012)
1761 [iis-8/installing-iis-8-on-windows-server-2012](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
1763 installed, follow the steps from this link to install SharePoint Server
1764 2013: [http://social.technet.microsoft.com/wiki/contents/articles/14209.sharepoint-2013-](http://social.technet.microsoft.com/wiki/contents/articles/14209.sharepoint-2013-installation-step-by-step.aspx)
1765 [installation-step-by-step.aspx](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
1770 **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.

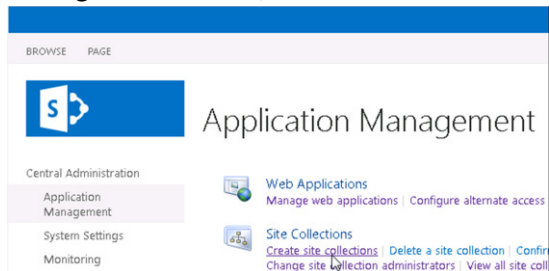
1775 Typically, you should accept the default path.

- 1776 5. In the Security Configuration section, you can leave the default options (Allow Anonymous=No,
1777 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.

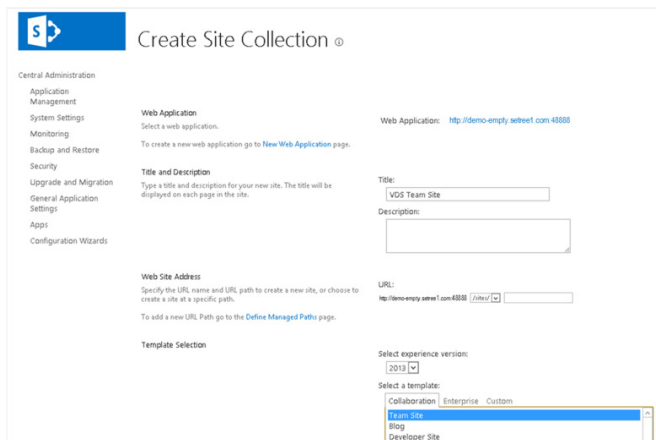
The screenshot shows the 'Security Configuration' dialog box. In the 'Claims Authentication Types' section, the 'Enable Forms Based Authentication (FBA)' checkbox is checked. Below this, the 'ASP.NET Membership provider name' text box contains 'VDSMembership' and the 'ASP.NET Role manager name' text box contains 'VDSRole'. Other options include 'Enable Windows Authentication' (checked), 'Integrated Windows authentication' (checked), 'Basic authentication (credentials are sent in clear text)' (unchecked), and 'Use Secure Sockets Layer (SSL)' (No).

- 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**.
 1793



- 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.
 1797

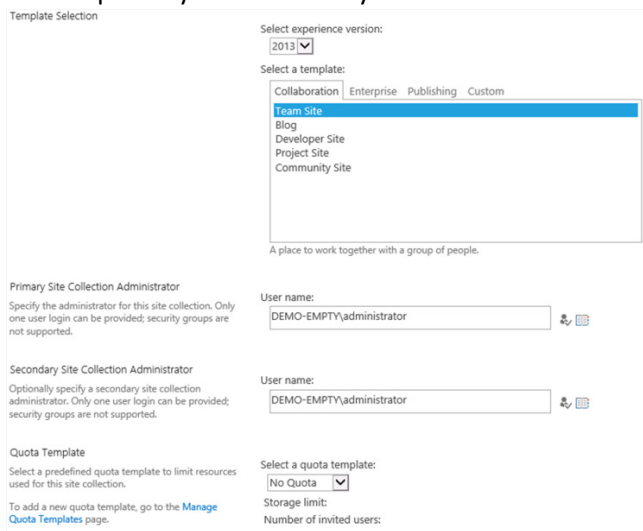
1798



1799

1800

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



1801

1802 2.7.6 Web Configs

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

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

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

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

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

DRAFT

```
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@nccoe1"
1827     useDNAttribute="false"
1828     userDNAttribute="distinguishedName"
1829     userNameAttribute="uid"
1830     userContainer="o=spusers1lam"
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=spgroups1lam"
1851     groupNameAttribute="cn"
```

DRAFT

```
1852     groupNameAlternateSearchAttribute="cn"
1853     groupMemberAttribute="member"
1854     userNameAttribute="uid"
1855     useUserDNAttribute="false"
1856     userContainer="o=spusers1lam"
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
1865 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=71e9bce111e9429c" />
1877 <add name="VDSMembership"
1878 type="Microsoft.Office.Server.Security.LdapMembershipProvider,
1879 Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
1880 PublicKeyToken=71e9bce111e9429c"
1881     server="192.168.14.111"
1882     port="2389"
1883     useSSL="false"
1884     connectionUsername="cn=Directory Manager"
1885     connectionPassword="Fsarm@ncceo1"
1886     useDNAttribute="false"
1887     userDNAttribute="distinguishedName"
```

DRAFT

```
1888         userNameAttribute="uid"
1889         userContainer="o=spusers1lam"
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=spgroups1lam"
1910         groupNameAttribute="cn"
1911         groupNameAlternateSearchAttribute="cn"
1912         groupMemberAttribute="member"
1913         userNameAttribute="uid"
1914         useUserDNAttribute="false"
1915         userContainer="o=spusers1lam"
1916         cacheDurationInMinutes="0"
1917         dnAttribute="distinguishedName"
1918         groupFilter="(ObjectClass=group) "
1919         userFilter="(ObjectClass=user) "
1920         scope="Subtree" />
1921 </providers>
1922 </roleManager>
```

DRAFT

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=spgroups1lam"
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"
```

DRAFT

```
1958     connectionUsername="cn=Directory Manager"
1959     connectionPassword="Fsarm@nccoe1 "
1960     useDNAttribute="false"
1961     userDNAttribute="distinguishedName"
1962     userNameAttribute="uid"
1963     userContainer="o=spusersllam"
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>
```

1978 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.

1981 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.

1986 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.

1989 Download Splunk Enterprise from 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:
- 1994 <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonWindows>
- 1995 • Command line:
- 1996 <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonWindowsviahecommandline>
- 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>

2001 2.8.3 Queries

2002 Splunk reports, alerts, and dashboards are powered by queries written in the Splunk Search Processing
 2003 Language (SPL). These queries are used to perform the analytics responsible for capturing events,
 2004 identifying trends, and detecting anomalies. Once a query is written, it can be saved as a report, an alert,
 2005 or as a dashboard panel. The following queries were also saved to dashboards to provide a central
 2006 viewing location for operators, managers, and decision makers.

2007 2.8.4 Query: Detect User Provisioning Accounts Events

2008 The following search query detects when a user account is provisioned or when the user account
 2009 attributes are modified. The provisioning and modification events detected include those that are in
 2010 compliance with the established workflow and originate from the approved provisioning system, as well
 2011 as those that violate the workflow. The output of the query shows which events were authorized and
 2012 which were not.

```

2013 (index=main sourcetype="wineventlog:security" EventCode=5136 OR EventCode=4720) OR
2014 (index=sandbox sourcetype="alertstacticstest" OR sourcetype="RadiantSourceTest") 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+\s\w+\.cn:(?P<LDAP_UID>\w+\S\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+\s)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.\w+\s\w+\s\w+)"|rex "\-
2028 create\(\):User: (?P<AD_MSG>\w+\s\w+\s\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>\S+)"|rex
2033 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## 1: (?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>\S+\s*\S+)"|rex
2036 "\<givenName>(?P<GivenName>\S+\s*\S+)<\|/givenName>"|rex
2037 "\<sn>(?P<SurName>\S+\s*\S+)<\|/sn>" |rex
2038 "\<employeeNumber>(?P<EmployeeNumber>\S+\s*\S+)<\|/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=="RadiantOne
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,"%RadiantOne VDS%"),"RadiantOne VDS","NULL") |eval
2058 host2=if(Like(host,"%WIN%"),"AlertE","NULL") |eval Authority=if((host1=="RadiantOne
2059 VDS" AND host2=="AlertE"),"Authorized", "Not Legal") |eval
2060 Authority=if((host1=="RadiantOne 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%")

```

2068 2.8.5 Query: Authorized and Unauthorized Provisioning Trend Line Chart

2069 The following search query generates a line chart showing the trends for both the authorized and
 2070 unauthorized provisioning events:

```

2071 earliest="1/25/2017:00:00:00" latest="2/15/2017:00:00:00" index=sandbox
2072 sourcetype="alertstatiectest" OR sourcetype="RadiantSourceTest" |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>\S+)" |rex
2082 "departmentNumber: (?P<DeptNumber>\w+)" |rex "## 1: (?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+\s*\S+)" |rex
2085 "\<givenName>(P<GivenName>\S+\s*\S+)<\givenName>" |rex
2086 "\<sn>(P<SurName>\S+\s*\S+)<\sn>" |rex
2087 "\<employeeNumber>(P<EmployeeNumber>\S+\s*\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

```

2117 2.8.6 Query: Combined Provisioning Trend Line Chart

2118 The following search query generates a line chart that shows the total authorized and unauthorized
 2119 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+\s\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>\S+)"|rex
2130 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## 1: (?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>\S+\s*\S+)"|rex
2133 "\<givenName>(P<GivenName>\S+\s*\S+)\</givenName>"|rex
2134 "\<sn>(P<SurName>\S+\s*\S+)\</sn>" |rex
2135 "\<employeeNumber>(P<EmployeeNumber>\S+\s*\S+)\</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 RLIICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLIICHANGES)|eval
2152 UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
2153 CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLIICHANGES
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 RLIICHANGETYPE RLIICHANGES EmpNo F_Name L_Name LDAP_UID
2159 AD_UID|where isnotnull(EmpNo)|table _time host Authority RLIICHANGETYPE RLIICHANGES
2160 EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority !="Not Legal"|eval
2161 CHANGES=if(isnotnull(RLIICHANGES),RLIICHANGES,RLIICHANGES)|eval
2162 CHANGETYPE=if(isnotnull(RLIICHANGETYPE),RLIICHANGETYPE,RLIICHANGETYPE)|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

```

2165 2.8.7 Query: Detect modifications to High Value or Privileged Accounts

2166 The following search query detects any modification to high-value accounts or privileged accounts, such
 2167 as managers and system administrators. It detects modifications that violate corporate policy as well as
 2168 those that are performed in accordance to policy.

```

2169 (index=main sourcetype="wineventlog:security" EventCode=5136 OR EventCode=4720) OR
2170 (index=sandbox sourcetype="alertstacticstest" OR sourcetype="RadiantSourceTest") OR
2171 (index=main sourcetype="openldap-outlog")|rex "givenName:(?P<FirstName>\w+)"|rex
2172 "sn:(?P<LastName>\w+)"|rex mode=sed "s/;/ /g"|rex
2173 "changetype:(?P<RLIICHANGETYPE>\w+)"|rex "employeeNumber:(?P<EmployeeNumber>\w+)"|rex
2174 "changetype:modify (?P<CHANGE>.+)"|rex "conn=\d+\s\w+\.cn=(?P<LDAP_UID>\w+\S\w+)"|rex
2175 "A user account was (?P<RLIICHANGETYPE>\w+)"|rex "A directory service object was
2176 (?P<RLIICHANGETYPE>\w+)"|eval
2177 RLIICHANGETYPE=if(RLIICHANGETYPE=="modified","update",RLIICHANGETYPE)|eval
2178 RLIICHANGETYPE=if(RLIICHANGETYPE=="created","insert", RLIICHANGETYPE)|eval
2179 RLIICHANGETYPE=if(RLIICHANGETYPE=="add","insert",RLIICHANGETYPE)|fields _time host
2180 checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
2181 RLIICHANGETYPE employeeNumber givenName sn uid gidnumber RLIICHANGES LDAP_UID LDAP_MSG
2182 AD_UID AD_MSG |rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex "\-create\(\):User:
2183 (?P<AD_UID>\w+\s)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.\w+\s\w+\s\w+)"|rex "\-
2184 create\(\):User: (?P<AD_MSG>\w+\s\w+\s\w+)" |rex
2185 "<RLIICHANGETYPE>(P<RLIICHANGETYPE>\w+)"|rex
2186 "<RLIICHANGES>(P<RLIICHANGES>.+)<\/RLIICHANGES>"|rex "employeeNumber:
2187 (?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
2188 (?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\S+)"|rex
2189 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## 1: (?P<L>\w+)"|rex "## o:
2190 (?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
2191 "mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\S+\s*\S+)"|rex
2192 "\<givenName>(P<GivenName>\S+\s*\S+)<\/givenName>"|rex
2193 "\<sn>(P<SurName>\S+\s*\S+)<\/sn>" |rex
2194 "\<employeeNumber>(P<EmployeeNumber>\S+\s*\S+)<\/employeeNumber>" |table _time
2195 host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
2196 RLIICHANGETYPE RLIICHANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
2197 LDAPUserId |where (isnotnull(FirstName)) OR (isnotnull(RLIICHANGES) OR
2198 (isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG))) OR isnotnull(RLIICHANGETYPE)|eval
2199 F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
2200 EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
2201 LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID) |table
2202 _time host checkStatus EmpNo F_Name L_Name RLIICHANGETYPE RLIICHANGES checkAuthFields
2203 LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLIICHANGES=if(RLIICHANGETYPE=="insert","New User
2204 Record",RLIICHANGES)| eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
2205 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%"))

```

2226 2.8.8 Query: Virtual Directory Server Offline Detection

2227 The following search query detects when the virtual directory server goes offline. The virtual directory
 2228 server is configured to send online status messages to Splunk at regular intervals. This query searches
 2229 for those messages and declares the virtual directory server offline if the last online message received
 2230 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

```

2235 2.8.9 Query: Critical Servers Offline

2236 The following search query detects when a directory server goes offline. The query uses the results of
 2237 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.slapped.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

```

2253 2.8.10 SSL Forwarding

2254 We took advantage Splunk's built in SSL forwarding capability and configured SSL encryption between
 2255 forwarders and the indexer. Instructions to enable SSL forwarding can be found at

2256 [http://docs.splunk.com/Documentation/Splunk/6.5.3/Security/ConfigureSplunkforwardingtousesignedc](http://docs.splunk.com/Documentation/Splunk/6.5.3/Security/ConfigureSplunkforwardingtousesignedcertificates)
2257 [ertificates.](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

DRAFT

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**.

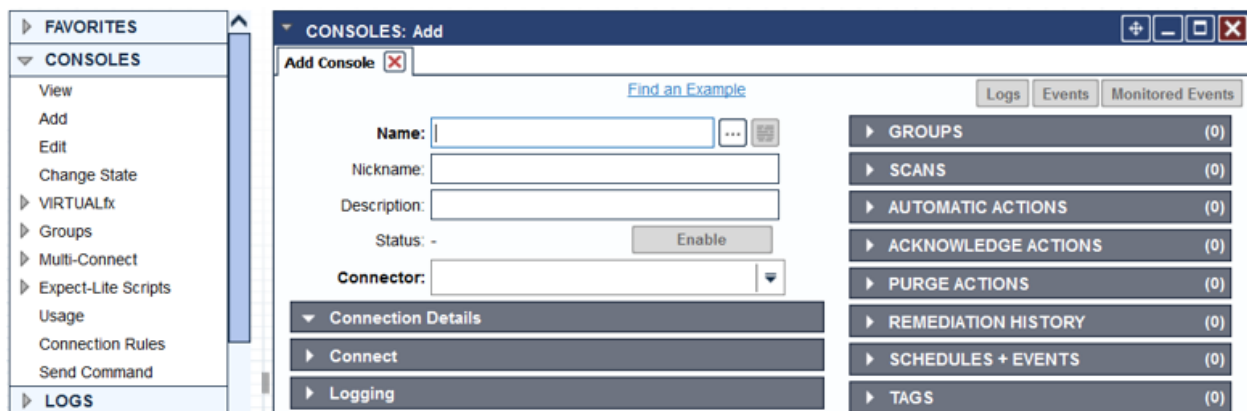
2304 2. Type in the name of the Console (for example, **OpenLDAPServer**).

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**.



2309

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.

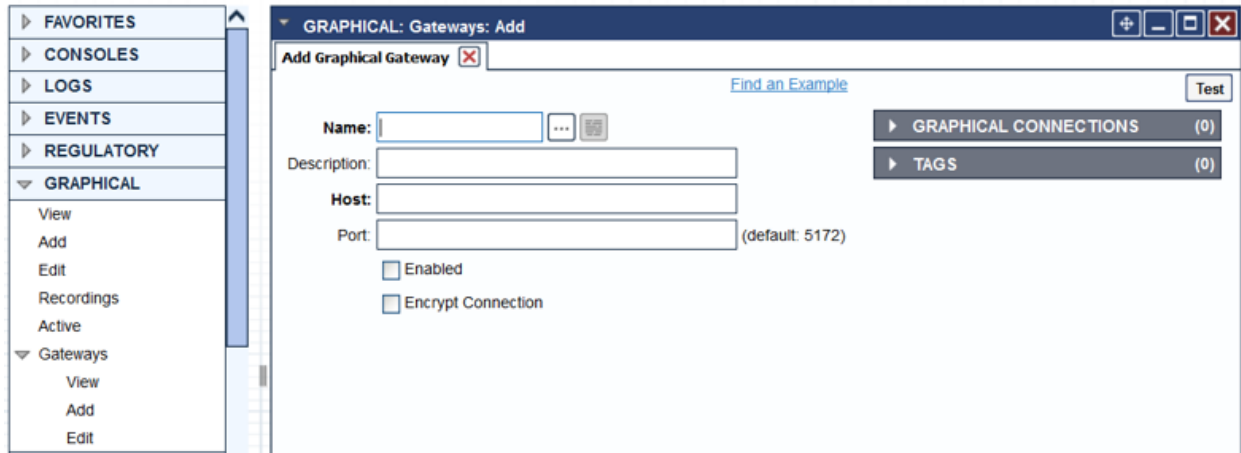
2315 `rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-version>.rpm`

2316 `/opt/gui_gateway/install_local.sh`

2317 `/opt/ConsoleWorks/bin/cw_start <invocation name> (created during installation)`

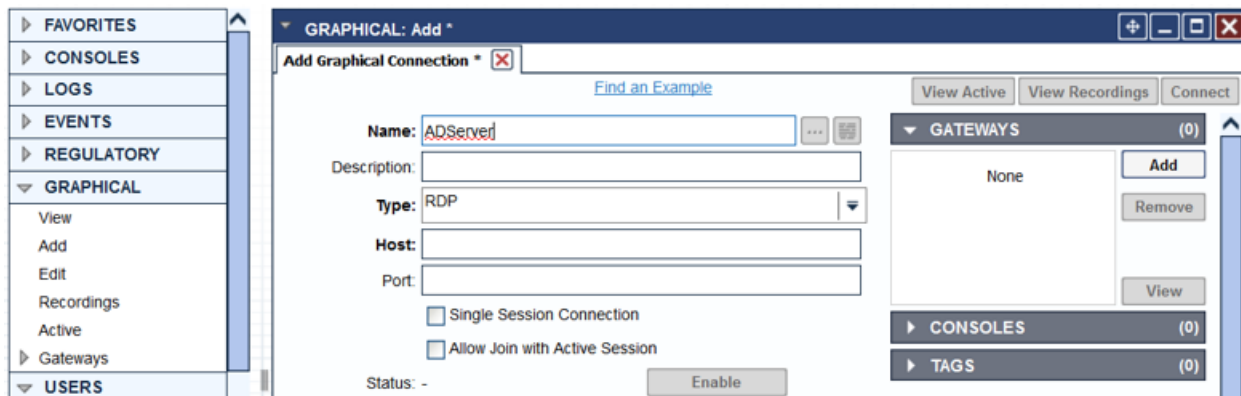
2318 `service gui_gatewayd start`

- 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.



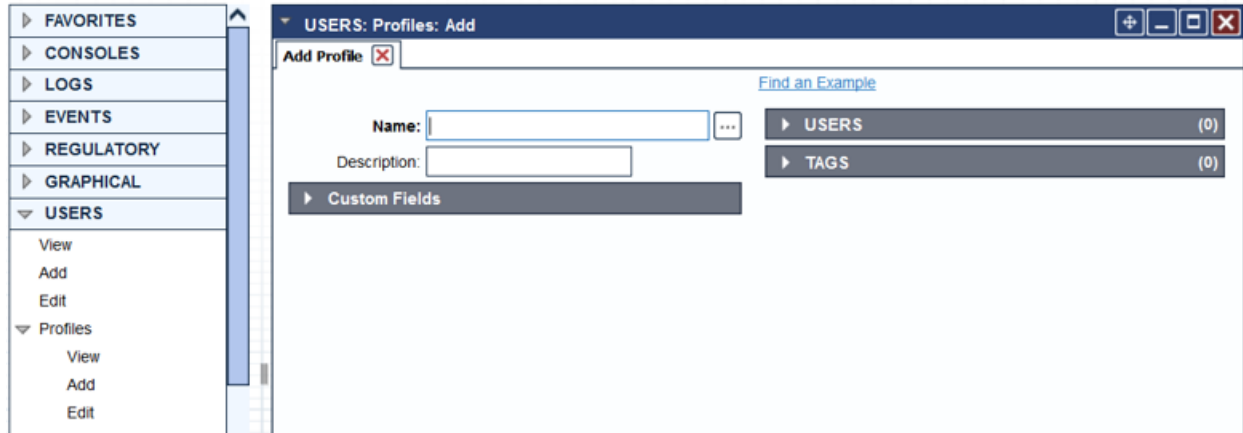
2324 2.9.7 Graphical Connection Configuration

- 2326 Configure the Graphical gateway:
- 2327 1. On the landing page of your ConsoleWorks server, click **GRAPHICAL>Add**.
 - 2328 2. Type in the name of the Graphical connection (for example, **ADServer**).
 - 2329 3. Choose a protocol in the **Type** drop-down list (for example, **RDP**).
 - 2330 4. Enter the name or IP address of the server in the **Host** field.
 - 2331 5. Type in the port number in the **Port** field. Enter **3389** for RDP.
 - 2332 6. Click **Save**.



2334 2.9.8 Profile Creation

- 2335 1. Click **USERS>Profiles>Add**.
- 2336 2. Type in the name of the profile in the **Name** field.
- 2337 3. Click **Save**.



2338

2339 2.9.9 Access Controls

2340 Access controls are rules that determine the level of access a user has to a Console or Graphical
 2341 connection. These rules can be associated with profiles and tags, which in turn can be associated with a
 2342 user to determine what a user has access to when logged in. In our build, we grouped privileged users
 2343 based on the servers they needed access to, created profiles that mirrored these groups, linked the
 2344 users to these profiles, and associated the access rules to the profiles.

2345 Create new access control rules:

- 2346 1. Copy the **CONSOLE_CONTROL** access control rule and assign it a number below 100. Access
 2347 control rules with lower numbers have priority over higher numbers.
- 2348 2. Select the newly copied access rule and click Edit.

SECURITY: Access Control: View

View Access Control Rules

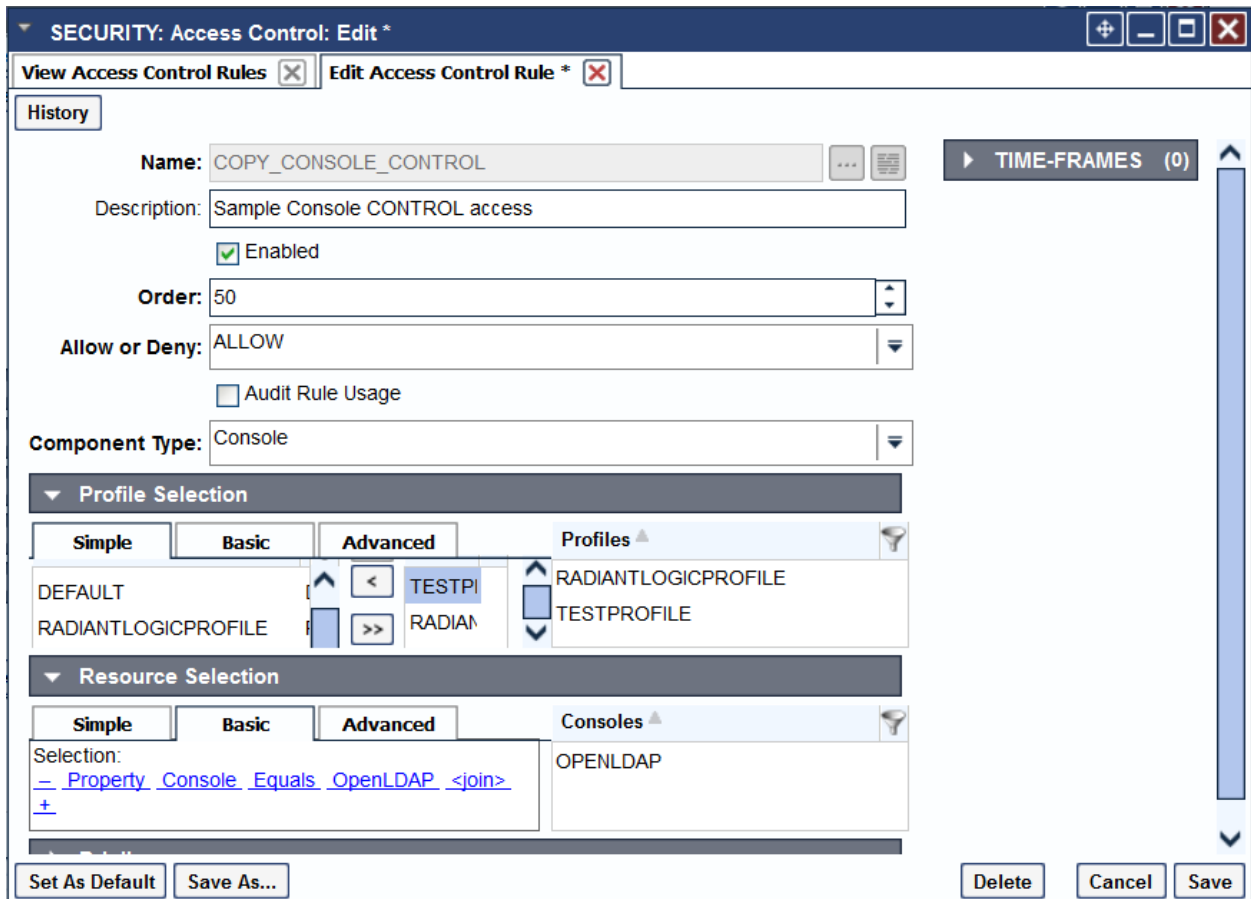
Order	Access Control Rule	Description	Enabled
<input type="checkbox"/>	48 COPY_CONSOLE_WRITE	Sample Console WRITE access	Y
<input type="checkbox"/>	49 COPY_CONSOLE_READ	Sample Console READ access	Y
<input checked="" type="checkbox"/>	50 COPY_CONSOLE_CONTROL	Sample Console CONTROL access	Y
<input type="checkbox"/>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

Buttons: Delete Add Examples Copy Rename Edit

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
- 2354 double arrows. Make sure it appears in the **Profiles** section.
- 2355 4. In the **Resource Selection** section, select the Console you want users associated with this profile
- 2356 to connect to. Select the **OpenLDAP** console.



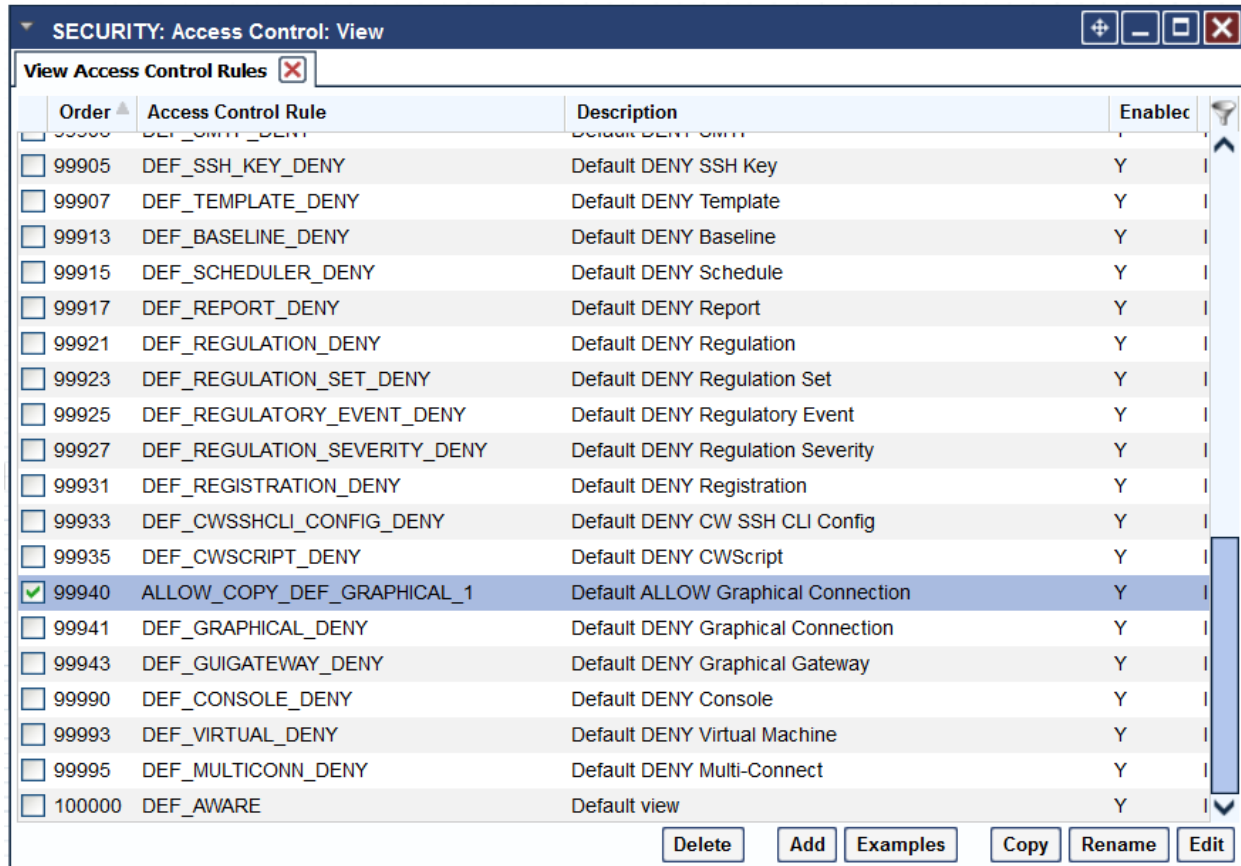
2357

2358

2359

2360

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



2361

2362

2363

2364

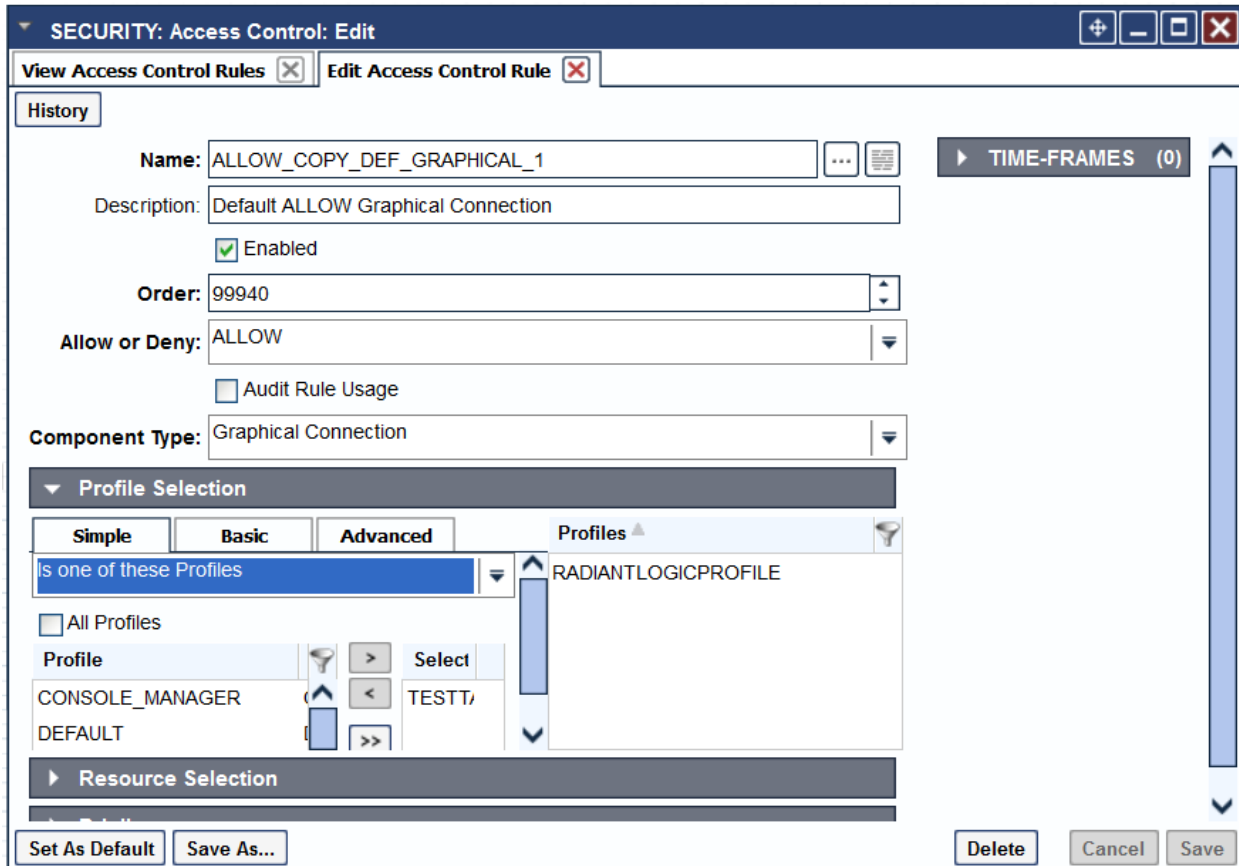
2365

2366

2367

2368

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



2369

2370

2371

1. Next, you will need to **Select** the Graphical Connection of choice such as RADIANTONE VDS.
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 / RADIAN

RADIANTONEVDS

TIME-FRAMES (0)

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.

The screenshot shows a web application interface for adding a user. On the left is a sidebar with a navigation menu. The main area is titled 'USERS: Add' and contains the following fields and sections:

- Name:** Text input field with a dropdown arrow.
- Description:** Text input field.
- Login Expiration:** Text input field with a calendar icon.
- User Created:** Text input field.
- Last Login:** Text input field.
- Use External Authentication**
- Password:** Section with a dropdown arrow, containing:
 - Password:** Text input field.
 - Retype Password:** Text input field.
 - Require Password Change On Next Login**
- Password Rules:** Section with a dropdown arrow.
- Contact Info:** Section with a dropdown arrow.

At the bottom of the form are buttons: 'Set As Default', 'Save As...', 'Change Password', 'Delete', 'Cancel', and 'Save'. A sidebar on the left shows a navigation menu with 'USERS' selected, and a list of sub-items including 'View', 'Add', 'Edit', 'Profiles', 'Change My Profile', 'Reset Passwords', 'Change Passwords', 'Change My Password', 'Preferences', 'Sessions', 'Send Message', and 'REPORTS'.

2379

2380 2.9.10 User Auditing

2381 An audit trail of ConsoleWorks user activity is captured in a file and forwarded to Splunk for further
 2382 analysis. The the information includes username, logon timestamp, and the target server to which the
 2383 user is connecting. The connection reporting script below parses the ConsoleWorks logs and writes the
 2384 output to a file. The bash connectionreporting script removes duplicate lines. The
 2385 bashconenctionreporting script is scheduled using cron to run every minute using the following
 2386 /etc/crontab configuration.

2387 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
```

2401 2.9.12 Scripts: connectionreporting

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

DRAFT

```
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)
```

2424 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
```

2432 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>$1$dSJmFph$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             <spoofofmac/>
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         </ipvnat>
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_57c017be3dff1.16882401</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>
```

DRAFT

```
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_57c017be3dff1.16882401</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>
```

DRAFT

```
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         <bypasststaticroutes>yes</bypasststaticroutes>
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         <uniqid>5804f45c4f196</uniqid>
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_sha1</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         <uniqid>586d5ecf7f516</uniqid>
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     <uniqid>586d5eeb02957</uniqid>
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         <uniqid>586d5f54943b4</uniqid>
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         <item>
4085             <minute>*/60</minute>
4086             <hour>*</hour>
4087             <mday>*</mday>
4088             <month>*</month>
4089             <wday>*</wday>
4090             <who>root</who>
4091             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4092 webConfiguratorlockout</command>
4093         </item>
4094         <item>
4095             <minute>1</minute>
4096             <hour>1</hour>
4097             <mday>*</mday>
4098             <month>*</month>
4099             <wday>*</wday>
4100             <who>root</who>
4101             <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
4102         </item>
4103         <item>
4104             <minute>*/60</minute>
4105             <hour>*</hour>
4106             <mday>*</mday>
4107             <month>*</month>
4108             <wday>*</wday>
4109             <who>root</who>
4110             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4111 virusprot</command>
4112         </item>
4113         <item>
4114             <minute>30</minute>
4115             <hour>12</hour>
4116             <mday>*</mday>
4117             <month>*</month>
```

```
4118         <wday>*</wday>
4119         <who>root</who>
4120         <command>/usr/bin/nice -n20 /etc/rc.update_urldata</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>
4186 </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     </cert>
4202     <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSB0tLS0tCk1JSUZiVENDQkZXZ0F3SUJBZ01CQURBTk1Jna3
4203 Foa2lHOXcwQkFRc0ZBREncdERFTE1Ba0dBmVVFQmhnQ1ZWtXgKRGpBTUJnTlZCQWdUQ1ZOMFlYUmxNUkV3RHdZ
4204 RFZRuUhfD2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApAvzV6W1NCM1pXSkRimjvtYVdkMWNtRjBiM0
4205 lnVTJWc1ppMVRhV2R1WldRZlEyVnlkR2xtYVdOaGRHVXhLREFTcKJna3Foa2lHOXcwQkNRRVdhV0ZrYltdsdVFI
4206 Qm1VMlZlYzJVdWJH0WpZV3hrYjIxaGFxNHhIakFjQmdOVk1JBTUQKRlhCbVUyVnVjMlV0TlRjeU1HRXdoVEF5WW
4207 pJM056QWVGdzB4TmBME1qY3hNVEU1TkRSYUz3MH1NVEV3TVRneApNVEU1TkRSYU1JRzBNUXN3Q1FZRFZRUUdF
4208 d0pWVXpFT01Bd0dBmVVFQ0JNR1UzUmhkr1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNU1UZ3dOZ1lEVLFRS0
4209 V5OXDabE5sYm50bE1IZGxZa052YmlacFozVnlZWfJ2Y2lCVFpXeG0KTFZocFoyNwxaQ0JEWlhKMGFXWnBZMkYw
4210 WlRfb01DWUdDU3FHU01iM0RRRUUpBUl1aWVdSdGFxNUFjR1pUWlcllegpaUzVzYjJOaGJHUNZiV0ZwYmpFZU1Cd0
4211 dBmVVFQXhNvMNHw1RaVzV6W1MwMU56SXdzVEExTURKaU1qYzNNSUlCCk1qQU5CZ2tXaGtpRz13MEJBUUUVGFUFP
4212 Q0FROEFNSUlCQ2dLQ0FRRU0L085aDlNt2R5R20yTnQ4R3dpUmw1bDAKVMz2NGJsQ2NwGjNYXFMUE1aVzNMDG
4213 hDODBHU0dhZnJENWdqctRwZkNMMH1zbEFPaV1Zk1hDYjdnA2o0dmtTMgpmBz14emNyaDURnV1aYlBHeXR1a21s
4214 ZWR4bjFwEFl6S1lZyXZkdn1Kb1lRMctNTkx0dkFjYnRhTUFoZjh1ZkRfClhrclNVQ0N5YTFrbEYxNWJGZmcyUG
4215 E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkuFRJTKx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
4216 ZEFiUEhjWgc5SFAONFQybfNIQ2M1cUp5UTdlK3IyaFZON29ENloXQmdCUApyeXdlSEZwd3J1LytYWExieEcrcD
4217 dwYXI0aHR0UFRDcm11NmFqQVVTNmpvN05kOE1QNWpZ1kzR0h2ZjhzUU1ECkFRQUJvNElCaGpDQ0FZSXdDUV1E
4218 V1IwVEJBSXdbREFSQmZz2hrZ0JodmhdQVFRUJBTUNCa0F3TXdZS1lJWkkKQV1iNFfnRU5CQ11XSku5d1pXNV
4219 RVMHdnUjJWdVpYSmhkr1ZrSUZObGNuWmxjaUJEWlhKMGFXWnBZMkYwW1RBZApCZ05WSFE0RUZnUVU3K11LRmNp
4220 OFFVSGhTZ0xEdjhfQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K11LcKzjaThRVUhoU2dMRHY4RUNzY0
4221 NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
4222 VUVCeE1JVEc5a1lXeHBkSGt4TORBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaqPRMj1lWm1sbmRYSmhkrZ15SU
4223 ZObGJHWRVmxuYm1Wa0lFTmxjblJwWm1sal1YUmxNU2d3SmdZSktvWklodmNOCkFra0JGagXoWkcxGjRQnda
4224 bE5sYm50bExtEHZMkZzWkc5dFlXbHVNUJR3SEFZRFZRUURFeFZ3WmxObGJUtmwKTFRVM01qQmhNRFV3TW1JeU
4225 56ZUNBUUF3SFFZRFZSMGxQ113RkFZSut3WUJCUVVIQXdFR0NDc0dBuVVGQ0FJQWpNQXNHQTFVZER3UUVBd01G
4226 b0RBTKJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZfPqDxd2MVZuUC82NmJDWFJ5CkVmaW1LRW1PcmtNaTB5M0
4227 9PWGtzWes1cEM2dtd6Ukl3WjEvRjYyRUp3OD1UOWx4Y01ZelZOTm5Idlg0bXfPRUCUWJhRU42NEkxOHFud3Zm
4228 S2JrREZvRThMR1hSdzBkMnAyTGVmYtd4YTIVSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTs9wV3p3aDdQRG
4229 c4bGdrCvc3dStlb01DNDJiIbVJkOURCTmlzdFJ4RVlNMkFLQkFsZG1LYStvRUY1VUwwCm43aXpvn1Z4dHJWMTJv
4230 TTdyS1lRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VnFULldDZGo3dDdIVG9ob0RFYzEKSk1kOVpPSmR2QmZLVU
4231 1sUW1ELyswSvpTa1FXRDczWkdsAehTK2tOewc1adJhUjUwYjhh3Wm9zQnNjSUZDa0pFbGp0UT09Ci0tLS0tRU5E
4232 IENFU1RJRklDQVRFLS0tLS0K</crt>
4233     <prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z01CQURBTk1Jna3Foa2lHOXcwQkFRRU
4234 ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M01hY1kKMjN3YkNKR1htWFJWky9odVVKeFdsc3hxb3M4
4235

```

```

4236 eGxiY3UyRUx6UVpJWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMwitqm0hOeXVIbjdsaGxzOG
4237 JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcWdTI4Qnh1CjFvdONGL3k1OE1SZVN0S1FJTEpyV1NVWFhs
4238 c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcWdkEKQVdEQkQzNDg5OHRUalhrOVNpb1NaclREbn
4239 dKTmo3cHAWQnM4ZHh1RDBjL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjv25DdTcvNWRj
4240 dhZFYjZudWxxdmlHMjA5TUtl1SzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWUW5L3l4QWdNQkFBRUNnZ0VCQUprRF
4241 pxU3duMnNTUTh0SVNBTUVrUW0zcXhrb3BzdZB4cWNScmFLOEd4VmQKejBpOU1KbkZVQWFleTQvL3JldndhZW1P
4242 R3RYSmZ2ai9jSnY3cmJIWGIzYkJtVW9hcDhxY0RjdnVSMm1HRUZyWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcD
4243 lzNVhhcHNpclNXVlI4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVdK1CjNLRmk4VTZUM1hnU1c2eFowZHp1ZnlP
4244 UzAvbXlmNU5YLzVoRklPNmFDc0xlUjZ4N1Rza2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
4245 hmZ0NRY1B2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtWnzhMY1FPMgppsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
4246 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUE0NzNMUWoxcExLSmRZN2JxCmtMU3NVTOZhTUZlZGlxU2ttbzh3Qj
4247 lpMXhzbElLQUd0M3U4dTdMz1ZtU2lybnMwVVBtMHRVUDRyQXMXVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
4248 OGttbFJnUFRmVHVPaGnWmGVkamQwK1E5Y2V1Y25kaFp3UE16TUc3TWRtSApKOG5yU2t5TFdMdWUxUVJNZNHhbm
4249 NBRdhVYThDZ1l1FQXpzYjYzbzRBSH1YNjZkEJ6TG1zYzZxS2d2ZG4xazhVCm02N3RuK2M3NkVhSEtZT1k0Rjdh
4250 S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNwVFTVVoZVo2OUpOK0I3Sm
4251 Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZmlDWlpRSUQ1OENnWUJjamFO
4252 dk5obnFJOG9rWGHBUjR2c3NtNgPwB0tYU1ZScjRIVHo5MDfWOGdReXNCWkt0CnlUS2V6VThuUVZvTjNYWmVMbC
4253 8rVEcwYVpKOTZHKy9nNTRWZmZqWTRle1VSChHUt3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
4254 QWY5Mi9CbHZJR25FSlpMdnhLWtdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
4255 VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGe0bU84WTBCEtNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
4256 RG1hZGsvKy9Ud2UvVklKbmX2TW9zS3VjTG42Y1c2eGVhR1hf3FoUj1hbkwzRjMKcEpUSGg4Y3FsnTdqdkRRN0
4257 FBamdyQmxb3pOvnNMZThiWWpkcHRLMVBRS0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1R1czdu
4258 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLC1UzSthhYnprnUUtWoeWzj
4259 VadTAxY1pZV5TU0FIUFRHYm5jb1IzbGVpYjNleUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
4260 OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>

4261     </cert>

4262     <revision>

4263         <time>1493217875</time>

4264         <description><![CDATA[admin@10.97.67.148: /firewall_nat_1to1_edit.php
4265 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         <uniqid>576b23658af3d</uniqid>
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         <uniqid>5773d4c39ae54</uniqid>
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         <uniqid>57a8ce7868f78</uniqid>
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         <uniqid>57aa0a09a4d09</uniqid>
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         <uniqid>57b615eac1f16</uniqid>
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         <uniqid>57bd089e9ab62</uniqid>
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         <uniqid>57bf0bbc594c5</uniqid>
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         <uniqid>57bf97481ae8c</uniqid>
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         <uniqid>581788c622d42</uniqid>
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         <uniqid>58179833f127e</uniqid>
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         <uniqid>58e410a9241f1</uniqid>
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         <uniqid>5900b1ef3b079</uniqid>
```

```

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>

```

4458 2.10.2 Firewall Configuration for Common Services Subnet

```

4459 <?xml version="1.0"?>
4460 <pfSense>
4461     <version>15.4</version>
4462     <lastchange/>
4463     <theme>pfSense_ng</theme>
4464     <system>
4465         <optimization>normal</optimization>
4466         <hostname>FS-ARM</hostname>
4467         <domain>FS-ARM.gov</domain>
4468         <group>
4469             <name>all</name>
4470             <description><![CDATA[All Users]]></description>
4471             <scope>system</scope>
4472             <gid>1998</gid>
4473             <member>0</member>
4474         </group>
4475         <group>
4476             <name>admins</name>
4477             <description><![CDATA[System Administrators]]></description>
4478             <scope>system</scope>
4479             <gid>1999</gid>
4480             <member>0</member>
4481             <priv>page-all</priv>
4482         </group>
4483         <user>
4484             <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         </rule>
4621     </filter>
4622 </config>
```

```
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_urltables</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<
5481 /sequence>
5482 </widgets>
5483 <openvpn/>
5484 <dnshaper>
5485 </dnshaper>
5486 <unbound>
5487     <enable/>
5488     <dnssec/>
5489     <active_interface/>
5490     <outgoing_interface/>
5491     <custom_options/>
5492     <hideidentity/>
5493     <hideversion/>
5494     <dnssecstripped/>
5495 </unbound>
5496 <dhcpdv6>
5497     <lan>
5498         <range>
5499             <from>::1000</from>
5500             <to>::2000</to>
5501         </range>
5502         <ramode>assist</ramode>
5503         <rapriority>medium</rapriority>
5504     </lan>
5505 </dhcpdv6>
```



```

5564 QWY5Mi9CbHZJR25FS1pMdnhLWTdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
5565 VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
5566 RG1hZGsvKy9Ud2UvVk1KbmX2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUj1hbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
5567 FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBRs0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1RlcZdu
5568 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLC1UzSThhYnpnUUtWoeWzj
5569 VadTAxY1pZVvk5TU0FIUFRHYm5jb1IzbGVpYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
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>

```

5600 2.10.3 Firewall Configuration for ID-ARM Subnet

DRAFT

```
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>$1$dSJmFph$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         <rule>
5841             <id/>
5842             <tracker>1493650861</tracker>
5843             <type>pass</type>
5844             <interface>wan</interface>
5845             <ipprotocol>inet</ipprotocol>
5846             <tag/>
5847             <tagged/>
5848             <direction>any</direction>
5849             <quick>yes</quick>
5850             <floating>yes</floating>
5851             <max/>
5852             <max-src-nodes/>
5853             <max-src-conn/>
5854             <max-src-states/>
5855             <statetimeout/>
5856             <statetype>keep state</statetype>
5857             <os/>
5858             <protocol>tcp/udp</protocol>
5859             <source>
5860                 <any/>
5861             </source>
5862             <destination>
5863                 <network>lan</network>
5864                 <port>389</port>
5865             </destination>
5866             <descr><![CDATA[Allow Connection to Port 389 in LAN]]></descr>
5867             <updated>
5868                 <time>1493650861</time>
5869                 <username>admin@10.97.67.135</username>
5870             </updated>
5871             <created>
5872                 <time>1493650861</time>
```

```
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_urltables</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             <ramode>assist</ramode>
6687             <rapriority>medium</rapriority>
6688         </lan>
6689     </dhcpdv6>
```



```

6748 QWY5Mi9CbHZJR25FS1pMdnhLWTdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
6749 VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
6750 RGlhZGsvKy9Ud2UvVk1Kbmx2TW9zS3VjTG42Y1c2eGvhR1hFc3FoUj1hbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
6751 FBamyQmxrb3pOVnNMZThiWWpkcHRlMVBRs0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1RlcZdu
6752 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLC1UzSThhYnpnUUtWoeWrZj
6753 VadTAxY1pZVv5TU0FIUFRHYm5jb1IzbGVpYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
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>

```

6842 2.10.4 Firewall Configuration for Private Cloud Subnet

```

6843 <?xml version="1.0"?>
6844 <pfSense>
6845     <version>15.4</version>
6846     <lastchange/>
6847     <theme>pfSense_ng</theme>
6848     <system>
6849         <optimization>normal</optimization>
6850         <hostname>FS-ARM</hostname>
6851         <domain>FS-ARM.gov</domain>
6852         <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             <spoofofmac/>
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>
```

DRAFT

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     7419     <sequence>system_information:coll:open,gateways:coll:open,interfaces:col2:open<
7420 /sequence>
7421     </widgets>
7422     <openvpn/>
7423     <dnshaper>
7424     </dnshaper>
7425     <unbound>
7426         <dnssec/>
7427         <active_interface>all</active_interface>
7428         <outgoing_interface>all</outgoing_interface>
7429         <custom_options/>
7430         <hideidentity/>
7431         <hideversion/>

```



```

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
7441      <enable/>
7442  </unbound>
7443  <dhcpdv6>
7444      <lan>
7445          <range>
7446              <from>::1000</from>
7447              <to>::2000</to>
7448          </range>
7449          <ramode>assist</ramode>
7450          <rapriority>medium</rapriority>
7451      </lan>
7452  </dhcpdv6>
7453  <cert>
7454      <refid>5720a0502b277</refid>
7455      <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
7456      <type>server</type>
7457      <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXXZ0F3SUJBZ0lCQURBTkJna3
7458      Foa2lHOXcwQkFRc0ZBREncdERFTE1Ba0dBMVVFQmhnNQ1ZWtXgKRGpBTUJnTlZCQWdUQ1ZOMFlYUmxNUkV3RHdZ
7459      RFZRUUhFd2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApVzV6W1NCM1pXSkRiMjVtYVdkMWNtRjBiM0
7460      lnVTJWc1ppMVRhV2RlWldRZlEyVnlkR2xtYVdOaGRHVXhLREFTcCkna3Foa2lHOXcwQkNRRVdHV0ZrY1dsdVFI
7461      Qm1VM1Z1YzJVdWJHOWpZV3hrYjIxaGFXNHhIakFjQmdOVk1JBTUQKRlhCbVUyVnVjM1V0T1RjeU1HRXdOVEF5WW
7462      pJM056QWVGdzB4Tm1qY3hNVEU1TkRSYU1TksYU1JRzBNUN3Q1FZRFZRUUdF
7463      d0pWVXpFT01Bd0dBMVVFQ0JNR1UzUmhkr1V4RVRBUEJnTlZCQWNUCkNFehZmZkZzYVhSNU1UZ3dOZ1lEVLFRS0
7464      V5OXDabE5sYm5ObE1lZGxZa052Ym1acFozVnlZWFFJ2Y2lCVFpXeg0KTFZocFoyNWxaQ0JEWlhKMGFXWnBZMkYw
7465      WlRFb01DWUdDU3FHU0liM0RRRUUpBUl1aWVdSdGFxNUFjR1pUW1clcgpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
7466      dBMVVFQXhNVMhNW1RaVzV6W1MwMU56SXZVEExTURKaU1qYzNNSU1CCk1qQU5CZ2tkaGtpRz13MEJBUUUVGQUFP
7467      Q0FR0EFNSU1CQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NwGJNYXFMUE1aVzNMdG
7468      hDODBHU0dhZnJENWdqTRwZkNNMH1zbEFpV1Zk1hdyjdNa2o0dmtTMgpm14emNyaDUrNV1aY1BHeXR1a21s
7469      ZWR4bjFwEFl6S1l1zYXZkdnlkbl1lRMCtNTkx0dkFjYnRhTUFoZjh1ZkRfClhrc1NVQ0N5YTFrbEYxNWJGZmcyUG
7470      E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkuFRJTKx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
7471      ZEFiUEhjWgc5SFA0NFQybfNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXdlSEZwd3Jl1YtYWExieEcrcD
7472      dwYXI0aHR0UFRDcm11NmFqQVVVNmpvN05kOE1QNWpZ1kzR0h2ZjhZUULECkFRQUJvNElCaGpDQ0FZSXdDUV1E
7473      VlIwVEJBSXdbREFSQmZ2hrZ0JodmhdQVFRUJBTUNCa0F3TXdZS1lJWkkKQV1iNFFnRU5CQ1lXSkU5d1pXNV
7474

```

7475 RVMHdnUjJwDvPYSmhkR1ZrSUzObGNuWmxjaUJUEWlhKMGFXWnBZMkYwWlRBZApCZ05WSFE0RUZnUVU3K11LRmNp
7476 OFFVSGhTZ0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K11LCkZjaThRVUhoU2dMRHY4RUNzY0
7477 NKd0FLaGdicWtnYmN3Z2JREn6QUpCZ05WQkFZVEFsV1RNUTR3REFZRFZRUUKRXdWVGRHRjBaVEVSTUE4R0Ex
7478 VUVCeE1JVEc5a1lXeHBkSGt4T0RBMkJnT1ZCQW9UTDNCbVUyVnVjM1VnZDJWaQpRMj1lWm1sbmRYSmhkRz15SU
7479 ZObGJHXRVMmxuYm1Wa01FTmxjblJwWm1sa1lYUmXNU2d3SmdZSkvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
7480 bE5sYm5ObExteHZZMkZzWkc5dF1XbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
7481 56ZUNBUUF3SFFZRFZSMGxCQ113RkFZSUt3WUJCUVVIQXdFR0NDc0dBUVVGG0FJQWpNQXNHQTFVZER3UUVBd01G
7482 b0RBTKJna3Foa21lHOXcwQkFRc0ZBQU9DQVFFQXJxZfPQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmtNaTB5M0
7483 9PWGtzWES1cEM2dTd6Uk13WjEvRjYyRUp3OD1UOWx4Y01ZelZOTm5Idlg0bXFPRUCKUWJhRU42NEKxOHFud3Zm
7484 S2JrREZvRThMR1hSdzBkMnAyTGVmYtd4YTIvSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTs9wV3p3aDdQRG
7485 c4bGdrcVc3dStlb01DNDJIBvJkOURCTmlzdfJ4RVlNMkFLQkFsZG1LYStvRUY1VUwwCm43aXpvn1Z4dHJWMTJv
7486 TTdySl1RQ05ky00xZkVSeUwvb3ZkUnVpa0F5Wm1VvNFULldDZGo3dDdIVG9ob0RFYzEKSklkVpPsmR2QmZLVU
7487 1sUW1ELyswSvpTalFXRDczWkdsAehTK2tOewc1aDjHujUwYj3h3Wm9zQnNjSUZDa0pFbpgp0UT09Ci0tLS0tRU5E
7488 IENFU1RJRklDQVRFLS0tLS0K</crt>

7489 <prv>LS0tLS1CRUDJTIBQUklWQVRFIETfWS0tLS0tCk1JSUV2Z01CQURBTkJna3Foa21lHOXcwQkFRRU
7490 ZBQVNDQktnd2dnU2tbZ0VBQW9JQkFRQzM4NzJIMkE1M01hY1lKkMjN3YkNKR1htWFJWky9odVVKefDsc3hxb3M4
7491 eGxiY3UyRUx6UVPjWnArclBtQ09yaWw4SXpUS3LVQTZKaG01YwpKdnN5U1BpK1JMWitqM0hOeXV1bjdsAGxzOG
7492 JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcWdtI4Qnh1CjFvdONGL3k1OE1SZVN0S1FJTTEpyV1NVWFhs
7493 c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcWdkEKQVdEQkQzNDG5OHRUalHROVnbp1Nac1REbn
7494 dKTmo3cHAWQnM4ZHh1RDBjL2poUGFWSWNKem1vbKpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjv25DdTCvNWRj
7495 dHZFYjZudWxxdmlHMjA5TUtlSzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUppRRF
7496 pxU3duMnNTUTh0SVNBTUVrUW0zcXhrb3BzdzB4cWNScmFlOEd4VmQKejBpOU1KbkZVQWFleTQvL3JldndhZW1P
7497 R3RYSmZ2ai9jSnY3cmJIWGIzYkjtVw9hcDhxY0RjdnVSMm1HRUZyWQpCL3hjNVpINT1aTUFabWE1VWVQLzNjC
7498 1zNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1Zn1P
7499 UzAvbXlmNU5YlZVoRklPNmFDC0xUjZ4N1Rza2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEedzVM0bXdyR2
7500 hMZ0NRY1B2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtwNzhMY1FPMgppsSGR5cTJxTmJsnDIwa3h5M2FnZ1F2
7501 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUe0NzNMUwocExLSmRZN2JxCmtMU3NVTOzhTUZlZGlxU2ttbzh3Qj
7502 lpMXhzbElLQUd0M3U4dTdMz1ZtU2lybnMwVVBtMHRVUDRYQXmZVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
7503 OGttbFJnUFRmVHVPaGNwMGVkamQwK1E5Y2V1Y25kaFp3UE16TUc3TWRtSApKOG5yU2t5TFdMdwUxUVJNZHNhbm
7504 NBRDhVYThDZ1lFQXpzYjYzYzZBSh1YNjZkcEJ6TG1zYzZxS2d2ZG4xazhVCm02N3RuK2M3NkVhSEtZT1k0Rjdh
7505 S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNwVFTVVoZVo2OUpOK0I3Sm
7506 Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZmlDWlpRSUQ1OENnWUJjamFO
7507 dk5obnFJOG9rWGHBUjR2c3NtNGpWb0tYU1ZScjRIVHo5MDFwOGdReXNCWkt0Cn1US2V6VThuUVZvtjNYWmVMbC
7508 8rVEcwYVpKOTZHKy9nNTRWZmZqWTR1elVSChhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSuc3
7509 QWY5Mi9CbHZJR25FSlpMdnhLWTdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWwNGL3hpdGJNTn
7510 VudmNUUjZxtZr0ekZtdG5TYWN3W1ftb2UvdUVIaGE0bU84WTBCeTNRcivitVU1BCCndVR2RiUnNhdTgxcU12VUtU
7511 RG1hZGsvKy9Ud2UvVk1Kbmx2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUj1hbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
7512 FBamdYQmxrb3pOVnNMZThiWWpkcHRlMVBRs0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoYQ1h1NE52K1l3a1R1czdu
7513 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqefEvSDgxMHRGd1p3cC9uSVdycnRCZ1ZLC1UzStHhYnprnUUtWOEwrZj
7514 VadTAXY1pZVvK5TU0FIUFRHYm5jblIzbGVPYjNleUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
7515 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>

```

7551 2.10.5 Firewall Configuration for the Management and Monitoring Subnet

```

7552 <?xml version="1.0"?>
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         <ip6nat>
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>
```

DRAFT

```
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_urldatales</command>
8458     </item>
8459 </cron>
8460 <wol/>
8461 <rrd>
8462     <enable/>
8463     <category>left=system-
8464 processor&right=&resolution=300&timePeriod=-
8465 ld&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:coll:open,gateways:coll:open,interfaces:col2:open<
8513 /sequence>
8514 </widgets>
8515 <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     <cert>
8544         <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSU0tLS0tCk1JSUZiVENDQkZXXZ0F3SUJBZ01CQURBTkNa3
8545 Foa2lHOXcwQkFRc0ZBREncdERFTE1Ba0dBMVVVFQmhnNQ1ZWtXgKRGpBTUJnTlZCQWdUQ1ZOMFlYUmxNUkV3RHdZ
8546 RFZRUUhFd2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApVzV6W1NCM1pXSkrImjvtYVdkMWNtrjBiM0
8547 lnVTJWc1ppMVRhV2R1WldRZlEyVnlkR2xtYVdOaGRHVXhLREFTcKJna3Foa2lHOXcwQkNRRVdhV0ZrYltdsdVFI
8548 Qm1VmlZlYzJVdWJHOWpZV3hrYjIxaGFXNHhIakFjQmdOVk1JBTUQKRlhCbVUyVnVjMlV0TlRjeU1HRXdOVEF5WW
8549 pJM056QWVGdzB4TnpBME1qY3hNVEU1TkRSYUZ3MH1NVEV3TVRneApNVEU1TkRSYU1JRzBNUNXN3Q1FZRFZRUUdF
8550 d0pWVXpFT01Bd0dBMVVVFQ0JNR1UzUmhkR1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNU1UZ3dOZ1lEVLFRS0
8551 V5OXdabE5sYm50bElIZGxZa052YmlacFozVnlZWfJ2Y2lCVFpXeg0KTFZ0cFoyNWxaQ0JEWlhKMGFXWnBZMkYw
8552 WlRFb01DWUdDU3FHU01iM0RRRUUpBUl1aWVdSdGFxNUFjR1pUW1c1egpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
8553 dBMVVVFQXhNVMNHw1RaVzV6W1MwMU56SXdZVEExtURKau1qYzNNSU1CCk1qQU5CZ2tXaGtpRz13MEJBUUVGQUFP
8554 Q0FROEFNSU1CQ2dLQ0FRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NwGJNYXFMUE1aVzNMdG
8555 hDODBHU0dhZnJENWdqctRwZkNNMH1zbEFPaV1ZK1hDYjdNa2o0dmtTMgpmbz14emNyaDURNVlaYlBHeXR1a21s
8556 ZWR4bjFwFwFl6S1lZyXZKdnlKb1lRMCtNTkx0dkFjYnRhTUfoZjh1ZkRfClhrclNVQ0N5YTFrbEYxNWJGZmcyUG

```


8557 E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkUFRJTKx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
8558 ZEFiUEhjWgc5SFAONFQybfNIQ2M1cUp5UTdlK3IyaFZON29ENloxQmdCUApyeXdlSEZwd3J1LytYWExieEcrcD
8559 dwYXI0aHR0UFRDcm11NmFqQVVTNmpvN05kOE1QNWpzZ1kzR0h2ZjhzUU1ECkFRQUJvNE1CaGpDQ0FZSXddUV1E
8560 V1IwVEJBSXdbREFSqmDsZ2hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZS1lJWkkKQVliNFFnRU5CQ1lXSkU5d1pXNV
8561 RVMHdnUjJWdVpYSmhkR1ZrSUZObGNuWmxjaUJEWlHKMGFXWnBZMkYwW1RBZApCZ05WSFE0RUZnUVU3K1lLRmNp
8562 OFFVSGhTZ0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K1lLcKzjaThRVUhoU2dMRHY4RUNzY0
8563 NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
8564 VUVCeE1JVEc5allXeHBkSGt4T0RBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaqPRMj1lWm1sbmRYSmhkRz15SU
8565 ZObGJHWXRVMmxuYm1Wa0lFTmxjblJwWm1sa1lYUmxNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
8566 bE5sYm50bExtEHZMkZzWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhnRFV3TW1JeU
8567 56ZUNBUUF3SFFZRFZSMGxCQl13RkFZSut3WUJCUVVIQXdfR0NDc0dBUVVGQ0FJQwpNQNHNQTFVZER3UUUVbd01G
8568 b0RBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZfPQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRW1PcmtNaTB5M0
8569 9PWGtzWES1cEM2dTd6Ukl3WjEvRjYyRUp3OD1UOWx4Y01Ze1ZOTm5Idlg0bXFPRUCUWJhRU42NEkxOHFud3Zm
8570 S2JrREZvRThMR1hSdzBkMnAyTGVmYtd4YTIVSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTS9wv3p3aDdQRG
8571 c4bGdrcVc3dStlB01DNDJIBvJKOURCTmlzdfJ4RV1NMkFLQkFsZG1LYStvRUy1VUwwCm43aXpvn1Z4dHJWMTJv
8572 TTdyS1lRQ05ky00xZkVSeUwvb3ZkUnVpa0F5Wm1VVnFULldDZGo3dDdIVG9ob0RFYzEKSklkOVpPsmR2QmZLVU
8573 1sUWlELyswSvpTa1FXRDczWkdsaEhTK2tOeWcladJhUjUwYj3hWm9zQnNjSUZDa0pFbpgp0UT09Ci0tLS0tRU5E
8574 IENFU1RJRklDQVRFLS0tLS0K</crt>

8575 <prv>LS0tLS1CRudJTibQUklWQVRFIETfWS0tLS0tCk1JSUV2Z0lCQURBTkJna3Foa2lHOXcwQkFRRU
8576 ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQZM4NzJIMke1M0lhY1kKMjN3YkNKr1htWFJWky9odVVKefDsc3hxb3M4
8577 eGxiY3UyRUx6UVPjWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMwitqM0hOeXVibjdsAGxzOG
8578 JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcWdTl4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEpyV1NVWFhs
8579 c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcWdkEKQVdEQkQzNDG5OHRUalhrOVNpb1Nac1REbn
8580 dKTmo3cHAWQnM4ZHh1RDBjL2poUGFWSWNKem1vbKpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjv25DdtcvNWRj
8581 dhZFYjZudWxxdmlHMjA5TUtlSzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUppRF
8582 pxU3duMnNTUTh0SVNBtUVrUW0zcxhrb3BzdzB4cWNScmFLOEd4VmQKejBpOU1KbkZVQWFleTQvL3JldndhZWlP
8583 R3RYSmZ2ai9jSnY3cmJIWGIzYkYtVW9hcDhxY0RjdnVSMmlHRUZyWQpCL3hjNvpINTlaTUFabWE1VWVQLzNjcd
8584 lzNVhchHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1ZnlP
8585 UzAvbXlmNU5YLzVoRklPNmFDC0x1UjZ4N1RZa2FDQU9FY1ViT29qUXkKc09XewphbEtTUWZ3WEdzdVM0bXdyR2
8586 hMZ0NRY1B2MnE5VONia0VMNEZUZmRzR1ZXcHBRNG1ZVWtwnzhMY1FPMgppsSGR5cTJxTmJsNDIwa3h5M2FnZ1F2
8587 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUe0NzNMUwoxcExLSmRZN2JxCmtMU3NVT0ZhtUZlZG1xU2ttbzh3Qj
8588 lpMXhzbElLQUd0M3U4dTdmZlZtU2lybnMwVVBtMHRVUDRyQXmzVfJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
8589 OGttbFJnUFRmVHPaGnWmgvKamQwK1E5Y2V1Y25kaFp3UE16TUc3TWRtSAPKOG5yU2t5TFdMdWUxUVJNZNHhbm
8590 NBRDhVYThDZ1lFQXpzYjYzbzRBSH1YNjZkEJ6TGlzYzZxS2d2ZG4axzhVcm02N3RuK2M3NkVhSEtZTlK0RjdH
8591 S0dFSklYeU0yQTJTe1Azdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNwVFTVVoZVo2OUpOK0I3Sm
8592 Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZm1DWlpRSUQ1OENnWUJjamFO
8593 dk5obnfJOG9rWghBUjR2c3NtNgPwb0tYU1ZScjRIVHo5MDfWOGdReXNCWkt0CnlUS2V6VThuUVzvTjNYWmVMbC
8594 8rVEcwYVpKOTZHKy9nNTRWzmZqWTRle1VSchHtU3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
8595 QWY5Mi9CbHZJR25FS1pMdnhLWtdVMXlIb1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
8596 VudmNUUjZxtZr0ekZtdG5TYWN3W1Ftb2UvdUVIaGe0bU84WTBCEtNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
8597 RG1hZGsvK9Ud2UvVklKbmx2TW9zS3VjTG42Y1c2eGvHr1hFc3FoUj1hbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
8598 FBandyQmxrb3pOVnNMZThiWWpkcHRlMVBRS0JnQ0xDR0R1RXNBjUxwZ1RtOG44bgoyQ1h1NE52K113a1R1czdu
8599 WjRoM3ZRODI1ZkQxbGvzVjBYdDJ1cVJqeFevSDgxMHRGd1p3c9uSVdycnRCZlZLClUzSthYnnpnUUtWOEwrZj
8600 VadTAXy1pZvk5TU0FIUFRHYm5jblIzbGVpYjNleUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
8601 OVFOVGJkQWJRci0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>

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             <uniqid>57bf05ffdcc3c</uniqid>
8636             <descr><![CDATA[VIP mapping to ConsoleWorks]]></descr>
8637             <type>single</type>
8638             <subnet_bits>32</subnet_bits>
8639             <subnet>192.168.13.171</subnet>
8640         </vip>
8641     </virtualip>
8642 </pfSense>
```

Appendix A List of Acronyms

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