

# 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 design that demonstrates ways in which a financial services  
3     company can improve their information and information system security by limiting employee  
4     access to only the information they need to do their job, at the time they need it, and nothing  
5     more. Essentially, enabling a company to give the right person the right access to the right  
6     resources at 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](https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf)



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

## SOLUTION

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

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

The NCCoE reference design includes the following capabilities:

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

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

## BENEFITS

The NCCoE's practice guide to address Access Rights Management for the financial services sector can help 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](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](mailto:financial_nccoe@nist.gov).

---

## 94      **TECHNOLOGY PARTNERS/COLLABORATORS**

95      Technology vendors who participated in this project submitted their capabilities in response to a call in the  
96      Federal Register. Companies with relevant products were invited to sign a Cooperative Research and  
97      Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this  
98      example implementation.

99      

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](mailto: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>

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

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

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

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

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

## ABSTRACT

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

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

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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

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

59 The technology vendors who participated in this build submitted their capabilities in response to a  
 60 notice in the Federal Register. Companies with relevant products were invited to sign a Cooperative  
 61 Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium  
 62 to build this example solution. We worked with:

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

## Contents

<b>1</b>	<b>Summary.....</b>	<b>8</b>
1.1	Challenge .....	8
1.2	Solution.....	9
1.3	Risk Considerations .....	10
1.4	Benefits.....	10
<b>2</b>	<b>How to Use This Guide.....</b>	<b>11</b>
2.1	Typographical Conventions .....	12
<b>3</b>	<b>Approach.....</b>	<b>13</b>
3.1	Audience .....	13
3.2	Scope .....	13
3.3	Assumptions.....	14
3.3.1	Security .....	14
3.3.2	Modularity.....	14
3.3.3	Human Resources Database/Identity Vetting.....	14
3.3.4	Technical Implementation .....	14
3.3.5	Limited Scalability Testing.....	15
3.3.6	Replication of Enterprise Networks.....	15
3.4	Risk Assessment.....	15
3.4.1	Assessing Risk Posture .....	15
3.4.2	Security Control Map .....	16
3.5	Security Functions and Subcategories Related to FFIEC.....	33
3.6	Technologies.....	36
<b>4</b>	<b>Architecture.....</b>	<b>41</b>
4.1	Architecture Description .....	41
4.1.1	High-Level Architecture .....	41
4.1.2	Reference Design.....	42
<b>5</b>	<b>Example Implementation.....</b>	<b>46</b>



91	5.1	Example Implementation Description.....	46
92	5.2	Operation of the Example Implementation .....	48
93	5.2.1	Example Implementation Network Components Overview .....	50
94	5.2.2	Common Services Network.....	52
95	5.2.3	Access Rights Management Network.....	52
96	5.2.4	Network Data Flows .....	53
97	5.3	Data .....	56
98	<b>6</b>	<b>Security Analysis.....</b>	<b>57</b>
99	6.1	Assumptions and Limitations.....	57
100	6.2	Build Testing.....	57
101	6.3	Scenarios and Findings .....	57
102	6.4	Analysis of the Reference Design’s Support for CSF Subcategories .....	58
103	6.4.1	Supported CSF Subcategories .....	63
104	6.5	Security of the Reference Design.....	71
105	6.5.1	Securing New Attack Surfaces.....	75
106	6.5.2	Ensuring Information Integrity .....	77
107	6.5.3	Privileged Access Management.....	77
108	6.5.4	Isolating Reference Design Capabilities from Each Other .....	78
109	6.5.5	Deployment Recommendations.....	80
110	6.6	Security Evaluation Summary.....	83
111	<b>7</b>	<b>Functional Evaluation.....</b>	<b>85</b>
112	7.1	ARM Functional Test Plan.....	85
113	7.2	ARM Use Case Requirements .....	86
114	7.3	Test Case: ARM-1 .....	91
115	7.4	Test Case ARM-2 .....	93
116	7.5	Test Case ARM-3 .....	95
117	7.6	Test Case ARM-4 .....	97
118	7.7	Test Case ARM-5.....	99
119		<b>Appendix A List of Acronyms.....</b>	<b>101</b>

120	<b>Appendix B Legend for Diagrams.....</b>	<b>102</b>
121	<b>Appendix C References .....</b>	<b>103</b>

## 122 List of Figures

123	Figure 4-1 ARM High-Level Architecture .....	41
124	Figure 4-2 ARM Reference Design .....	43
125	Figure 5-1 Example Implementation .....	47
126	Figure 5-2 Example Implementation Data Flow .....	49
127	Figure 5-3 Monitoring Data Flow .....	50
128	Figure 5-4 ARM Example Implementation Network .....	51
129	Figure 5-5 Common Services Network .....	52
130	Figure 5-6 ID-ARM Network .....	53
131	Figure 5-7 User Access Information Network Data Flow (Steps 1 and 2 in Figure 5-2) .....	54
132	Figure 5-8 User Access Information Network Data Flow (Step 3 in Figure 5-2) .....	55
133	Figure 5-9 Monitoring Network Data Flow.....	56

## 134 List of Tables

135	Table 3-1 ARM Reference Design CSF Core Components Map .....	18
136	Table 3-2 FFIEC CAT Guidance.....	33
137	Table 3-3 Products and Technologies.....	36
138	Table 5-1 Example Implementation Component List .....	46
139	Table 6-1 ARM Reference Design Capabilities and Supported CSF Subcategories.....	59
140	Table 6-2 Capabilities for Managing and Securing the ARM Reference Design .....	72
141	Table 7-1 Test Case Fields .....	86
142	Table 7-2 ARM Functional Requirements.....	87
143	Table 7-3 Test Case ID: ARM-1 .....	91
144	Table 7-4 Test Case ID: ARM-2 .....	93
145	Table 7-5 Test Case ID: ARM-3 .....	95
146	Table 7-6 Test Case ID: ARM-4 .....	97
147	Table 7-7 Test Case ID: ARM-5 .....	99

## 1 Summary

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

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

### 1.1 Challenge

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

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

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

## 1.2 Solution

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

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

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

This practice guide:

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

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

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

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

### 1.3 Risk Considerations

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

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

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

### 1.4 Benefits

The reference design and example implementation has the following benefits:

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

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

## 2 How to Use This Guide

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

This guide contains three volumes:

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

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

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

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

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

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

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

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

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

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

A *NIST Cybersecurity Practice Guide* does not describe "the" solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute comments using email [financial\\_nccoe@nist.gov](mailto:financial_nccoe@nist.gov) or online via the web content tool.

## 2.1 Typographical Conventions

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> .
<b>Bold</b>	names of menus, options, command buttons and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on- screen computer output, sample code examples, status codes	<code>mkdir</code>
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<b><code>service sshd start</code></b>
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a>



## 3 Approach

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

### 3.1 Audience

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

### 3.2 Scope

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

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

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

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

### 3.3 Assumptions

#### 3.3.1 Security

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

#### 3.3.2 Modularity

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

#### 3.3.3 Human Resources Database/Identity Vetting

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

#### 3.3.4 Technical Implementation

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

### 3.3.5 Limited Scalability Testing

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

### 3.3.6 Replication of Enterprise Networks

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

## 3.4 Risk Assessment

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

We performed two types of risk assessment:

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

### 3.4.1 Assessing Risk Posture

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

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

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

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

- undocumented accounts
- accounts with unnecessarily elevated privileges
- dependence on humans to enforce user access policies

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

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

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

### 3.4.2 Security Control Map

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

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

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

CSF Subcategory	NIST 800-53 rev4 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>ID.AM-3: Organizational communication and data flows are mapped.</b>	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.
<b>ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established.</b>	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 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>ID.BE-4: Dependencies and critical functions for delivery of critical services are established.</b>	SA-14, CP-8, PE-9, PE-11, PM-8, SA-14	A.11.2.2, A.11.2.3, A.12.1.3	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.	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.

CSF Subcategory	NIST 800-53 rev4 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>PR.AC-1: Identities and credentials are managed for authorized devices and users.</b>	AC-2, IA Family	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>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>	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><b>PR.AC-3: Remote access is managed.</b></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 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.</b>	AC-2, AC-3, AC-5, AC-6, AC-16	A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4	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.	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.

<b>PR.DS-1: Data-at-rest is protected.</b>	SC-28	A.8.2.3	<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><b>PR.DS-2: Data-in-transit is protected.</b></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 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
				IS.WP.I.4.1: Evaluate the appropriateness of technical controls mediating access between security domains.
<b>PR.DS-5: Protections against data leaks are implemented.</b>	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 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.</b>	AU Family IR-5, IR-6	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	D2.MA.Ma.B.1: Audit log records and other security event logs are reviewed and retained in a secure manner.	IS.B.79: Institutions should strictly control and monitor access to log files whether on the host or in a centralized logging facility. 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. 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.

CSF Subcategory	NIST 800-53 rev4 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality. (p. 29).</b>	AC-3, CM-7	A.9.1.2	<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><b>PR.PT-4:</b> <b>Communications and control networks are protected.</b></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 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
				<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 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</b>	AC-4, CM-2, SI-4	A.13.1.1, A.13.2.1	D3.DC.Ev.B.1: A normal network activity baseline is established.	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.
<b>DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.</b>	CA-7, IR-5, SI-4	A.12.4.1	D3.DC.Ev.E.1: A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).	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.

CSF Subcategory	NIST 800-53 rev4 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>DE.AE-5: Incident alert thresholds are established.</b>	IR-4, IR-5	A.12.4.1	<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 <sup>a</sup>	IEC/ISO 27001 <sup>b</sup>	FFIEC CAT v1 <sup>c</sup>	FFIEC IT Exam Handbook Information Security <sup>d</sup>
<b>DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.</b>	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.	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. IS.WP.II.M.1: Review security procedures for report monitoring to identify unauthorized or unusual activities. 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.

a. Mapping taken from “Framework for Improving Critical Infrastructure Cybersecurity,” NIST, February 12, 2014

b. Mapping taken from “Framework for Improving Critical Infrastructure Cybersecurity,” NIST, February 12, 2014

c. Mapping taken from FFIEC Cybersecurity Assessment Tool Appendix B, FFIEC, June 2015

d. Mapping taken from FFIEC Cybersecurity Assessment Tool Appendix A, FFIEC, June 2015

### 3.5 Security Functions and Subcategories Related to FFIEC

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

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

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

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

**Table 3-2 FFIEC CAT Guidance**

FFIEC CAT Guidance	ARM Solution Characteristics
<b>D4.C.Co.Int.1: A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.</b>	Data flows into and out of the ARM system are documented and enforced because of the asset value to the organization.
<b>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.</b>	The ARM system is classified as a critical asset that needs to be protected.
<b>D3.PC.AM.B.6: Identification and authentication are required and managed for access to systems, applications, and hardware.</b>	The ARM system manages the updates to the identity and authentication systems (directories) using automation to ensure access policy compliance.
<b>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.</b>	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><b>D3.PC.Am.B.15:</b> Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication.</p> <p><b>D3.PC.Im.Int.2:</b> Security controls are used for remote access to all administrative consoles, including restricted virtual systems.</p> <p><b>D3.PC.Am.B.1:</b> Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.</p> <p><b>D3.PC.Am.B.2:</b> Employee access to systems and confidential data provides for separation of duties.</p> <p><b>D3.PC.Am.B.5:</b> 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><b>D3.PC.Am.Int.1:</b> 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><b>D3.PC.Am.B.13:</b> Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet).</p> <p><b>D3.PC.Am.E.5:</b> Controls are in place to prevent unauthorized access to cryptographic keys.</p> <p><b>D3.PC.Am.Int.7:</b> Confidential data is encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.</p> <p><b>D3.PC.Im.B.1:</b> Network perimeter defense tools (e.g., border router and firewall) are used.</p> <p><b>D3.PC.Im.Int.1:</b> 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><b>D2.MA.Ma.B.1:</b> 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><b>D3.PC.Am.B.4:</b> User access reviews are performed periodically for all systems and applications based on the risk to the application or system.</p> <p><b>D3.PC.Am.B.3:</b> 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><b>D4.RM.Om.Int.1:</b> Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.</p> <p><b>D3.DC.Ev.E.1:</b> A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).</p> <p><b>D5.DR.De.B.1:</b> Alert parameters are set for detecting information security incidents that prompt mitigating actions.</p> <p><b>D3.DC.An.E.4:</b> Thresholds have been established to determine activity within logs that would warrant management response.</p> <p><b>D3.DC.An.Int.3:</b> Tools actively monitor security logs for anomalous behavior and alert within established parameters.</p> <p><b>D3.DC.An.A.3:</b> 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>	

### 3.6 Technologies

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

**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	<a href="#">RadiantOne VDS</a> 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	<a href="#">Guardian</a>	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	<a href="#">Guardian</a>	4.0 SP04 HF3	Provisions access authorizations from the ARM workflow to Active Directory, OpenLDAP, and Vanguard
	Centralized provisioning of access information		Provisioning	AlertEnterprise	<a href="#">Guardian</a>	4.0 SP04 HF3	Provisions access authorizations from the ARM workflow to Active Directory, OpenLDAP, and Vanguard
	User access information repository		Directory	AlertEnterprise	<a href="#">Guardian</a>	4.0 SP04 HF3	Maintains the authoritative source for user access information
				Microsoft	<a href="#">Active Directory</a>		User access information repository
				OpenLDAP	<a href="#">OpenLDAP</a>		User access information repository
			Mainframe RACF interface	Vanguard Integrity Professionals	<a href="#">Vanguard</a>		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	<a href="#">Console Works</a>	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	<a href="#">CloudControl</a>		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	<a href="#">Console Works</a>	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	<a href="#">Console Works</a>	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	<a href="#">Enterprise</a>	6.4	Records logs from all systems to monitor for anomalous personnel activity.
			Privileged User Access Management	TDi Technologies	<a href="#">Console Works</a>	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	<a href="#">Enterprise</a>	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	<a href="#">Enterprise</a>	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	<a href="#">Console Works</a>	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	<a href="#">Enterprise</a>	6.4	Records logs for analysis and correlation.

## 4 Architecture

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

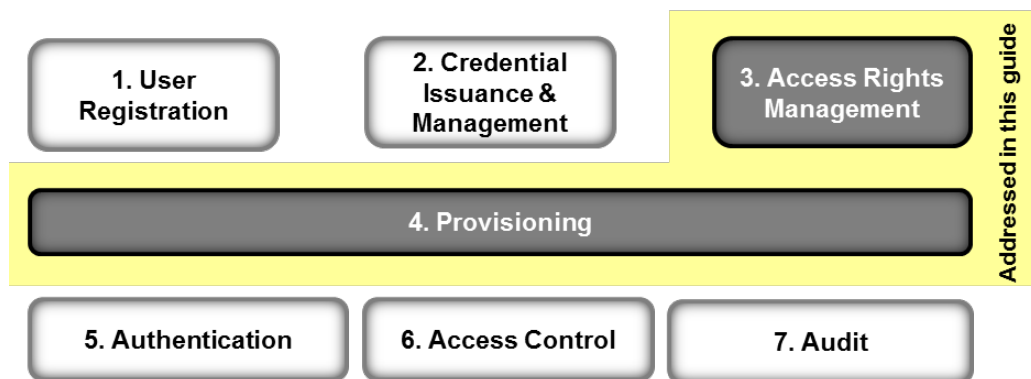
This section describes the high-level architecture and reference design for the ARM system.

### 4.1 Architecture Description

#### 4.1.1 High-Level Architecture

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

Figure 4-1 ARM High-Level Architecture



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

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

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

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

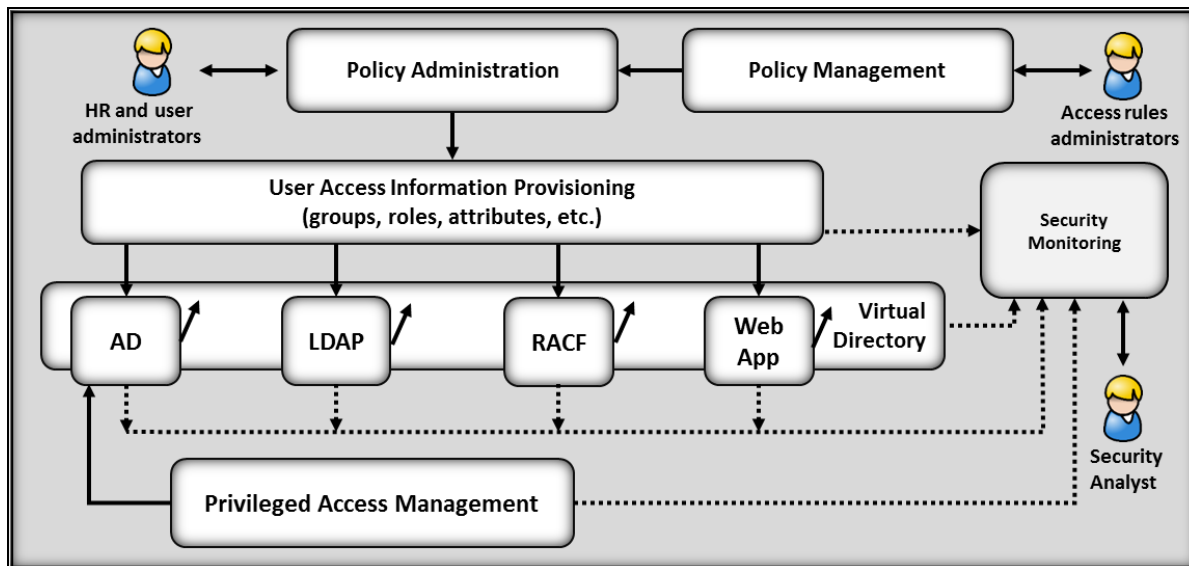
Directories, such as Microsoft Active Directory (AD), Resource Access Control Facility (RACF), and OpenLDAP, are often used in the implementation of run-time functions. Companies typically maintain multiple directories based on application needs and business acquisitions/combinations. These directories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

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

#### 4.1.2 Reference Design

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

Figure 4-2 ARM Reference Design



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

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

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

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

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

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

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

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

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

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



569 administrators do not need to make changes to the directories except for limited situations using the  
570 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

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

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

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

## 5 Example Implementation

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

### 5.1 Example Implementation Description

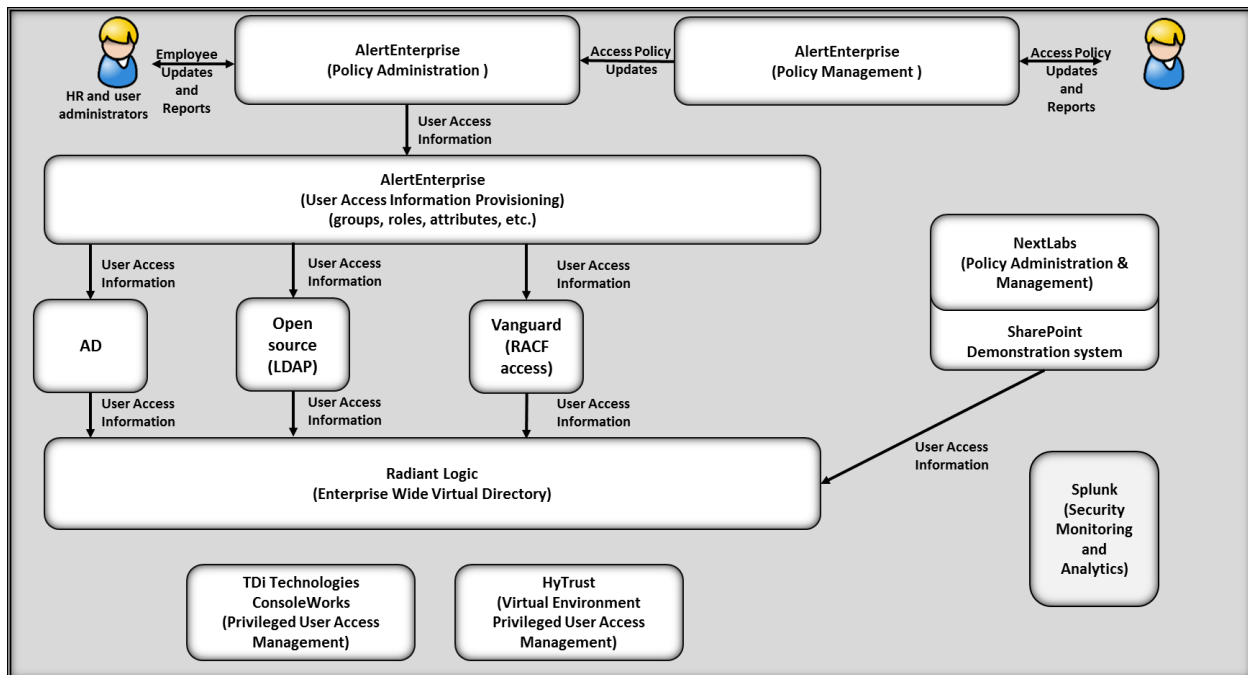
The example implementation is constructed on the NCCoE lab's infrastructure, which consists of a VMware vSphere virtualization operating environment. We used network-attached storage and virtual switches to interconnect the solution components as well as Internet access. The lab network is not connected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

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

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

Figure 5-1 illustrates the example implementation.

Figure 5-1 Example Implementation



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

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

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

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

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

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

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

## 5.2 Operation of the Example Implementation

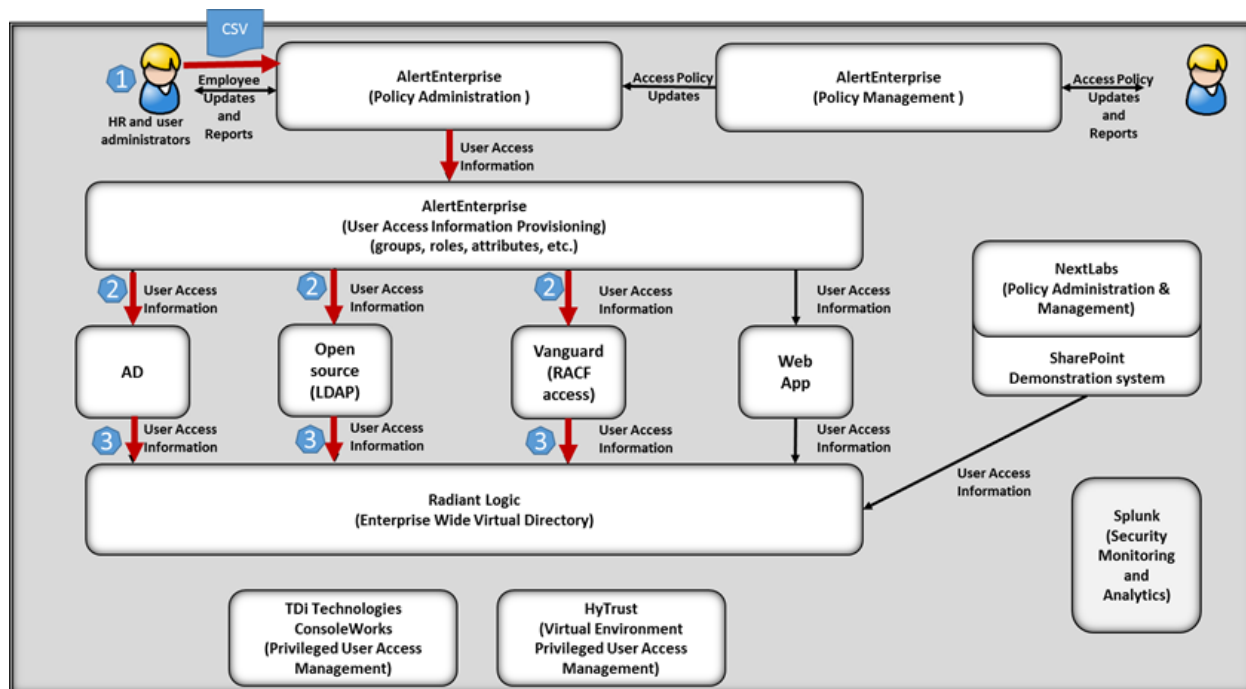
This section explains how the example implementation addresses the risk functions identified in [Section 3.4.1](#). Those factors include inability to centrally manage user accounts and inability to provision, modify, or revoke access throughout the enterprise in a timely manner.

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

The operation of the solution has three primary steps:

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

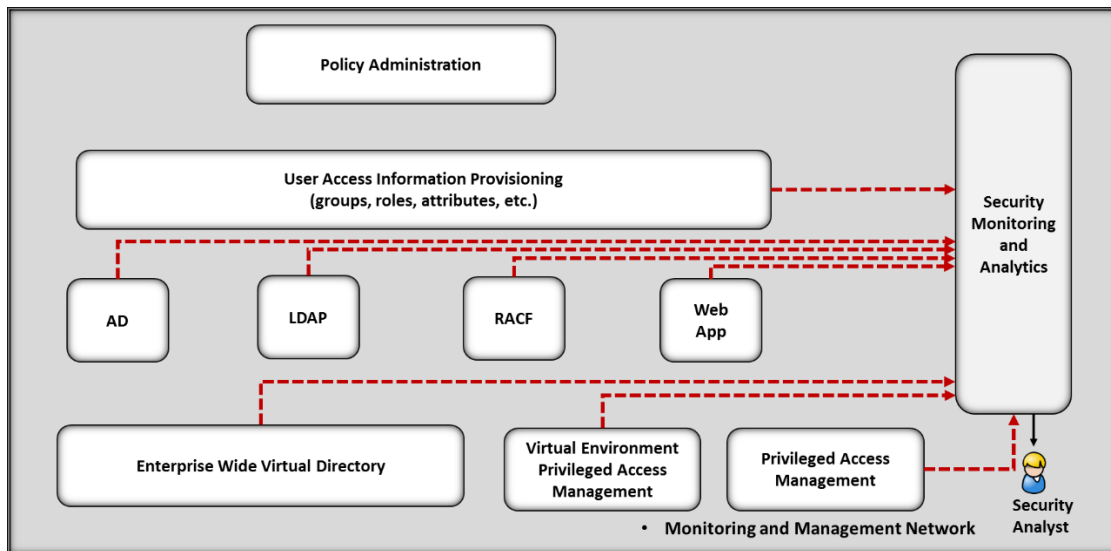
Figure 5-2 Example Implementation Data Flow



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

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

Figure 5-3 Monitoring Data Flow



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

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

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

### 5.2.1 Example Implementation Network Components Overview

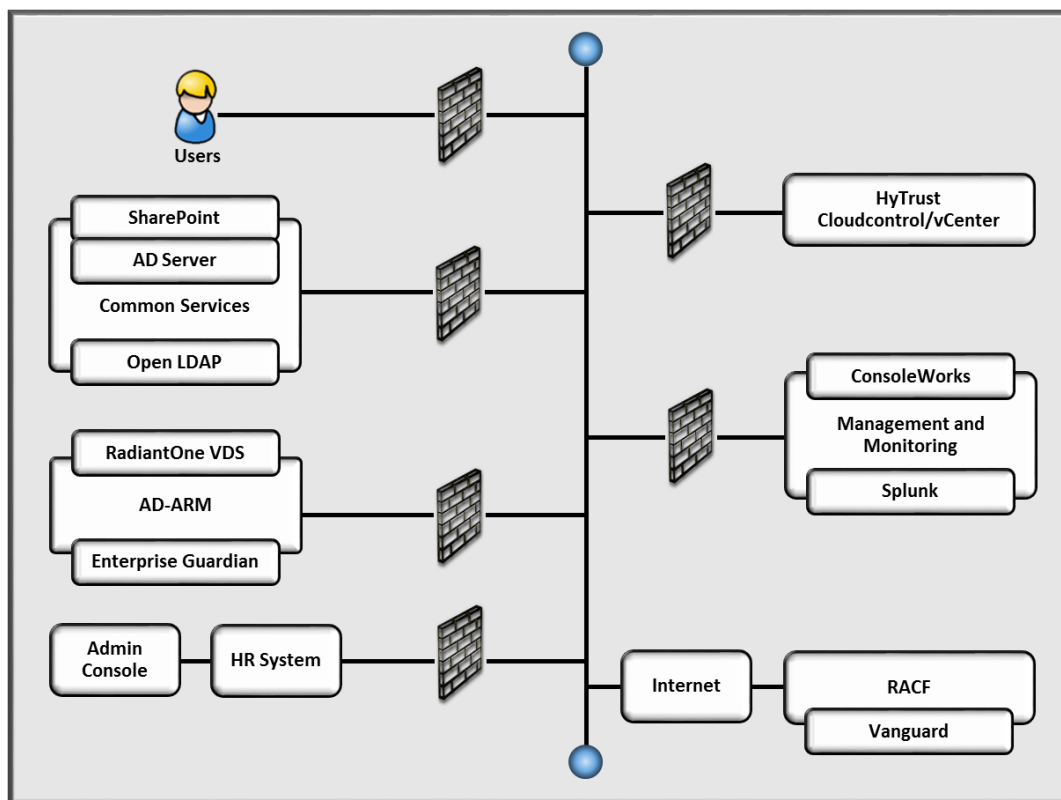
The example implementation architecture consists of multiple networks that partially mirror the infrastructure of a typical financial services company. A management network was implemented to facilitate the management and monitoring of the systems. The example implementation consists of the following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

- common services
- access rights management (ID-ARM)
- end-user systems

- virtual environment management
- users
- management and monitoring
- HR
- backbone

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

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



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

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

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

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

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

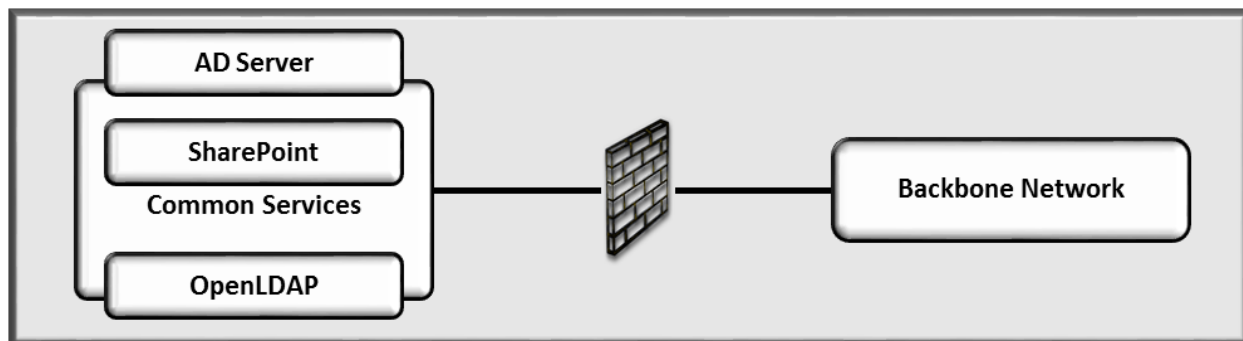
### 5.2.2 Common Services Network

The example implementation includes the following common services components:

- Active Directory
- OpenLDAP directory
- SharePoint servers

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

**Figure 5-5 Common Services Network**



### 5.2.3 Access Rights Management Network

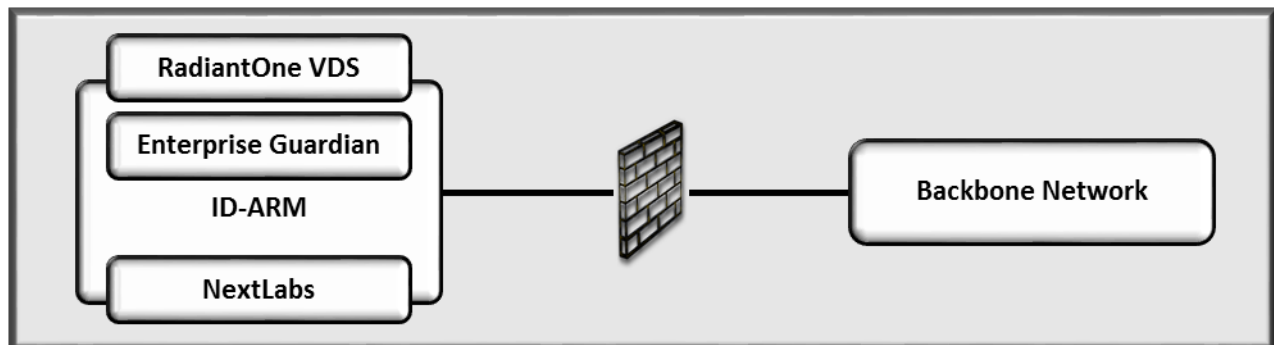
The following products were installed on the ARM network

- AlertEnterprise Enterprise Guardian ARM system
- Radiant Logic RadiantOne Virtual Directory
- NextLabs Entitlement Management

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



Figure 5-6 ID-ARM Network



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

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

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

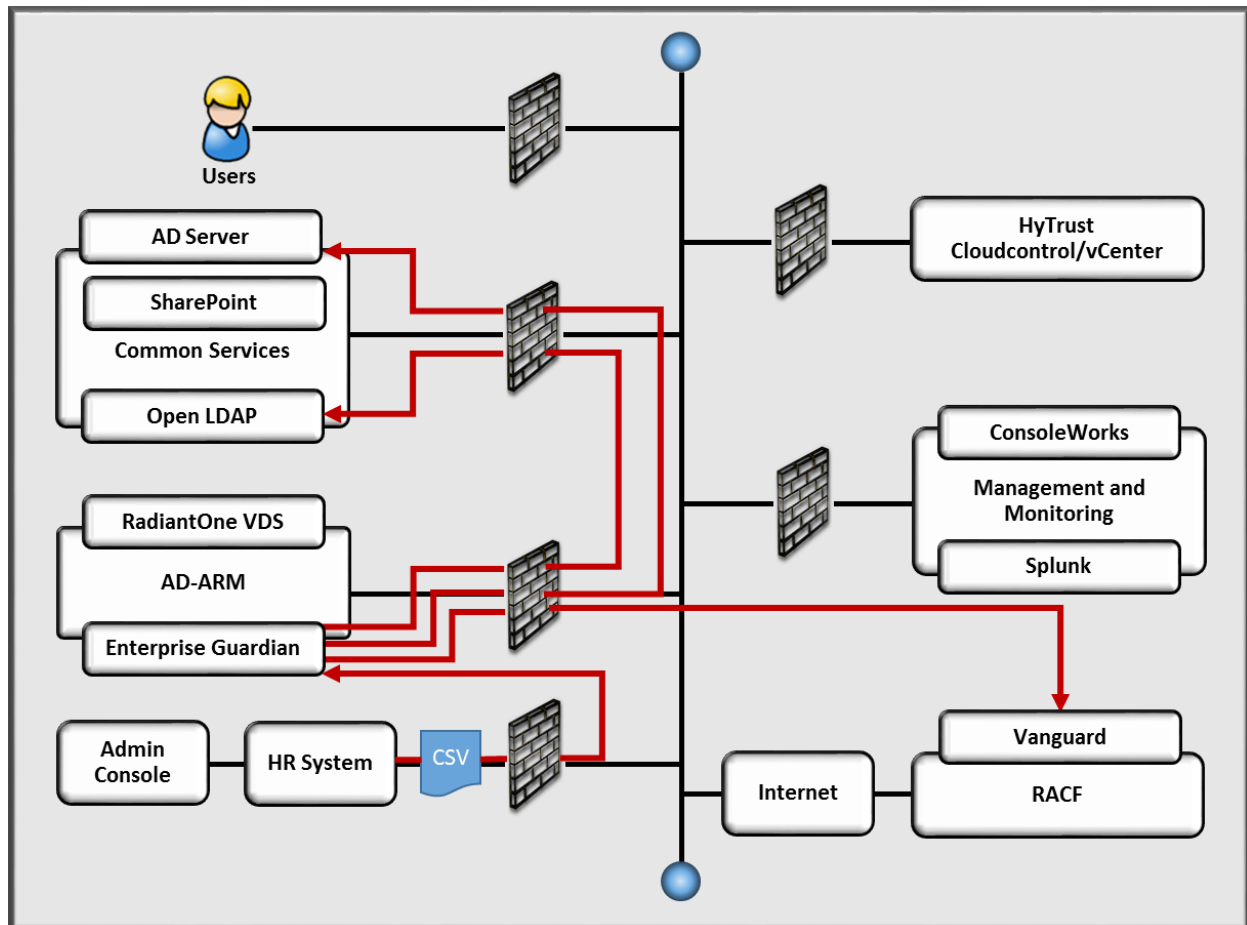
The NextLabs Entitlement Management product provides the attribute-based access control capability for an instance of SharePoint. The NextLabs product provides the policy decisions for SharePoint when determining access rights for any user attempting to log in to a SharePoint site. This functionality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

#### 5.2.4 Network Data Flows

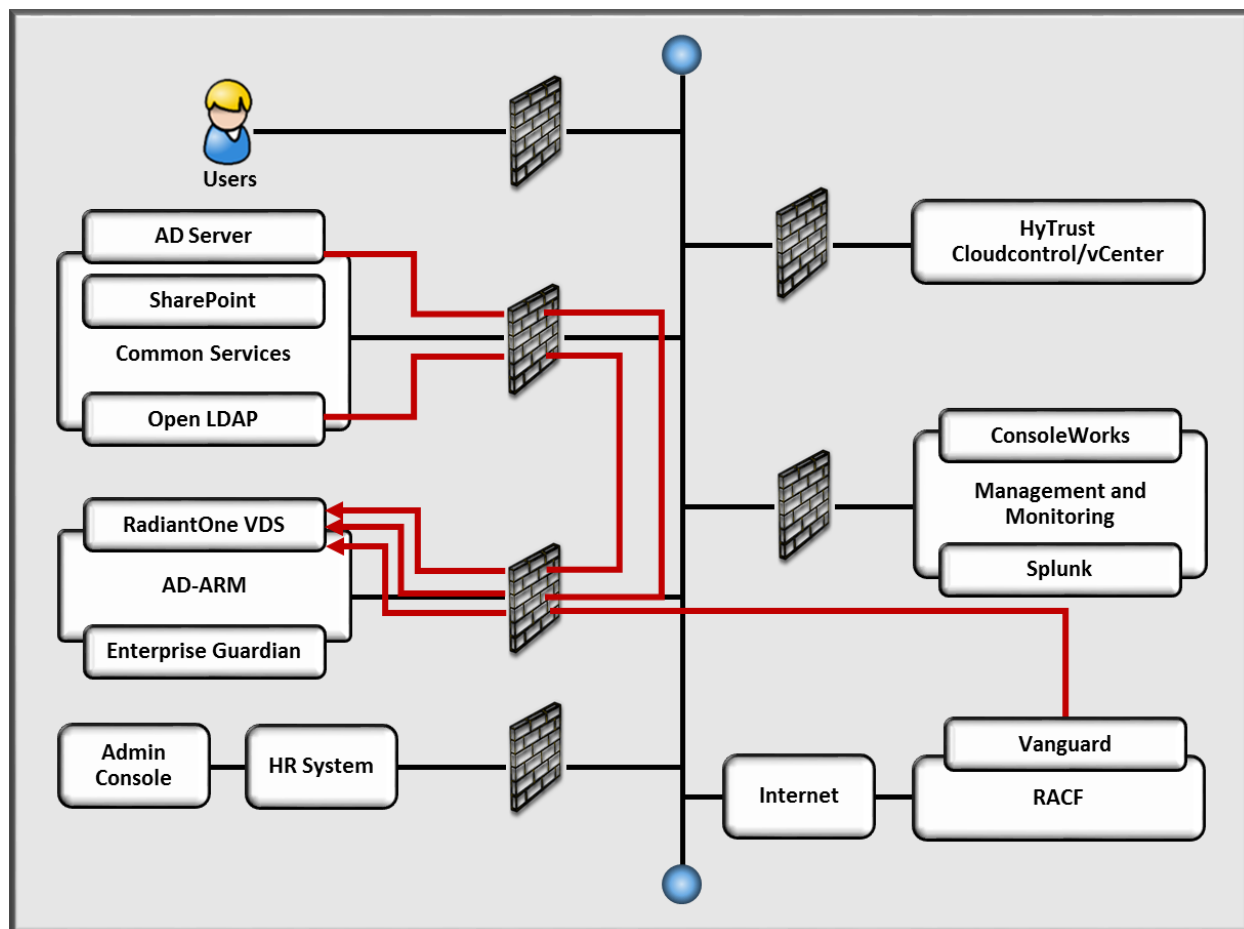
This section describes the data flows within the networks implemented in the example implementation. Figures 5-7 and 5-8 depict data flows using red lines with arrows indicating the flow direction superimposed on network diagrams. The steps are described in [Section 5.1](#). Figure 5-7 depicts the flow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

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

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



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



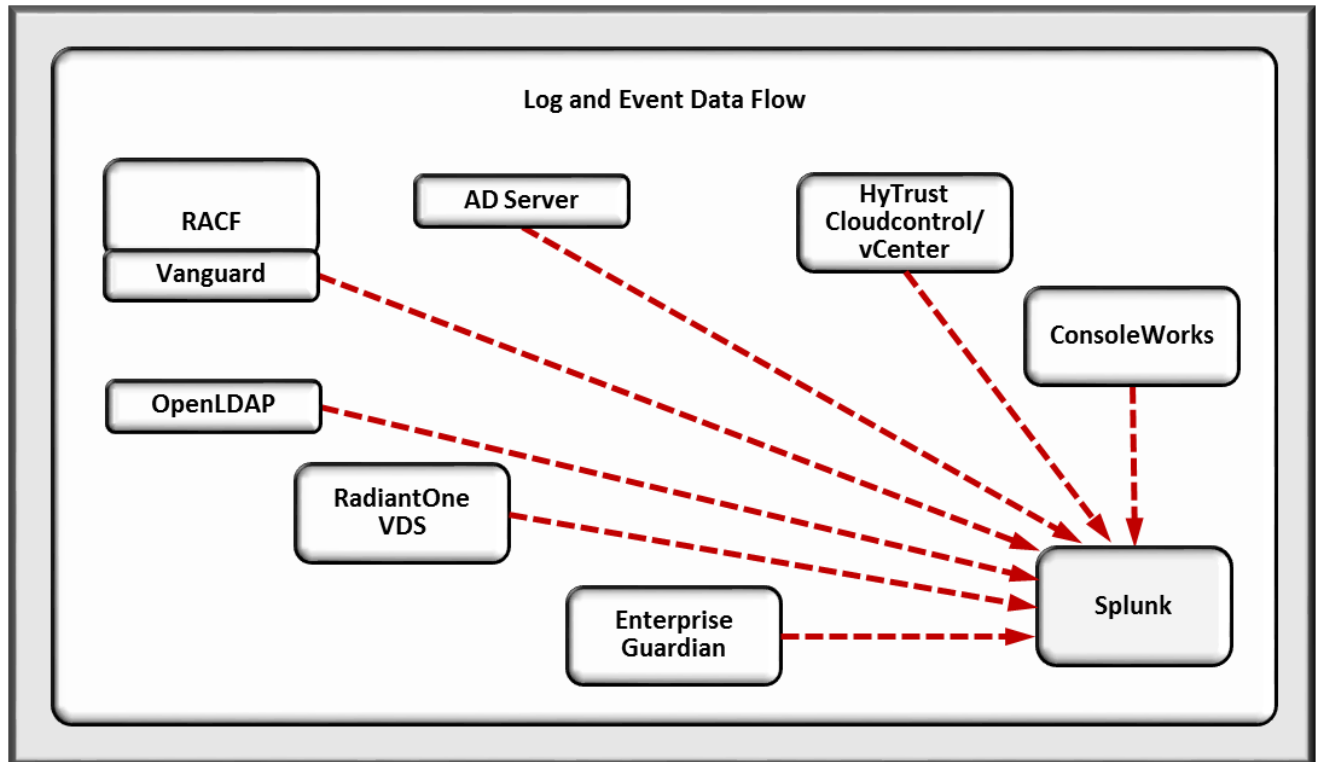
763

764 The system monitoring data (log and event data) flow occurs between each system and the security

765 monitoring system. Figure 5-9 depicts the data flows. All monitoring and management data are sent via

766 a separate management network segregated from the Backbone (production) network.

Figure 5-9 Monitoring Network Data Flow



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

### 5.3 Data

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

## 6 Security Analysis

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

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

### 6.1 Assumptions and Limitations

The security evaluation has the following limitations:

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

### 6.2 Build Testing

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

### 6.3 Scenarios and Findings

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

## 6.4 Analysis of the Reference Design's Support for CSF Subcategories

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

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

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

Capability	Specific Product	Function	CSF Subcategories
<b>Policy Management</b>	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.
<b>Policy Administration</b>	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.
<b>User Access Information Provisioning</b>	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
<b>User Access Information Repository (also referred to as Directory)</b>	Active Directory OpenLDAP Vanguard	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.	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.
<b>RACF Interface</b>	Vanguard	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.	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.



Capability	Specific Product	Function	CSF Subcategories
<b>Enterprise-wide Virtual Directory</b>	RadiantOne VDS	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.	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
<b>Security Monitoring and Analytics (also referred to as Monitoring)</b>	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.

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

## 6.4.1 Supported CSF Subcategories

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

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

The reference design:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

1109 are not authorized are attempted. The Security Monitoring capability monitors the alerts generated by  
 1110 these physical and virtual PAM capabilities to detect potential cybersecurity events.

## 1111 **6.5 Security of the Reference Design**

1112 The list of reference design capabilities in Table 6-1 focuses on the access control capabilities of the  
 1113 reference design that are needed to enable it to meet its objective of automating the management of  
 1114 user access information (accounts). Table 6-1 does not focus on capabilities needed to manage and  
 1115 secure the reference design. However, the reference design itself must be managed and secured. To this  
 1116 end, this second part of the security evaluation focuses on the security of the reference design.

1117 Measures implemented to protect the reference design from outside attack include:

- 1118     ▪ isolating certain capabilities on separate subnetworks protected by firewalls
- 1119     ▪ implementing a management network to isolate log and management traffic from the  
 1120       production (business operations) networks
- 1121     ▪ securing critical user access information and logs to protect them from unauthorized insertion,  
 1122       modification, or deletion
- 1123     ▪ logging of all privileged user access activities
- 1124     ▪ encryption and integrity protection of user access information and logs while this information is  
 1125       in transit between capabilities

1126 Table 6-2, Capabilities for Managing and Securing the ARM Reference Design, describes the security  
 1127 protections each capability provides and lists the corresponding products that were used to instantiate  
 1128 each capability. The security evaluation focuses on the capabilities rather than the products. The NCCoE  
 1129 is not assessing or certifying the security of the products included in the example implementation. We  
 1130 assume that the enterprise already deploys network security capabilities such as firewalls and intrusion  
 1131 detection devices that are configured according to best practices. The focus here is on securing  
 1132 capabilities introduced by the reference design and minimizing their exposure to threats.

1133 **Table 6-2 Capabilities for Managing and Securing the ARM Reference Design**

1134 This table describes only the product capabilities and CSF subcategory support used in the reference architecture. Many of the products have  
 1135 significant additional security capabilities that are not listed here.)

Capability	Specific Product	Function	CSF Subcategories
<b>Subnetting</b>	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.
<b>User Access Information Repository Firewall</b>	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
<b>Privileged Access Management</b>	TDi Technologies ConsoleWorks	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.	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.
<b>Virtual Environment Privileged Access Management</b>	HyTrust Cloud Control	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.	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.

Capability	Specific Product	Function	CSF Subcategories
<b>Log Integrity</b>	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. 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>

1136

### 6.5.1 Securing New Attack Surfaces

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

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

#### 6.5.1.1 Securing Access to the Policy Administration Capability

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

#### 6.5.1.2 *Securing Access to the Policy Management Capability*

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

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

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

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

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

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



## 6.5.2 Ensuring Information Integrity

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

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

## 6.5.3 Privileged Access Management

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

### 6.5.3.1 Privileged Users

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

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

### 6.5.3.2 *Insider Threat*

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

### 6.5.3.3 *Privileged User Access Information Storage*

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

### 6.5.4 *Isolating Reference Design Capabilities from Each Other*

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

- 1276       ▪ Policy Administration, Policy Management, User Access Information Provisioning, and Virtual
- 1277       Directory capabilities
- 1278       ▪ Security Monitoring and Analytics capability and Privileged Access Management capability
- 1279       ▪ Virtual Environment Privileged Access Management capability
- 1280       ▪ Directories

1281 Each of the reference design subnetworks is also isolated, via subnetting, from the enterprise's  
1282 production network (backbone network).

1283 Each subnetwork is separated from the rest of the reference design by a firewall that is configured to  
1284 restrict the type of data that flow into and out of the subnetwork to the minimum set of necessary  
1285 protocols. The ports and protocols to which each firewall restricts access are documented in NIST SP  
1286 1800-9C: *How-To Guides*.

#### 1287 *6.5.4.1 Addressing Attacks*

1288 We used the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) model and  
1289 framework developed by The MITRE Corporation to identify the following adversary tactics and  
1290 techniques that the reference design protects against:

- 1291       ▪ Privilege escalation results when an adversary obtains a higher level of permissions on a system  
1292       or network than he is authorized to have.
- 1293       • An adversary employing the tactic of privilege escalation might use the technique of trying  
1294       to modify his user access information attributes that are stored in the enterprise  
1295       directories so that these attributes permit him to have more access authority than he is  
1296       entitled.

1297 The reference design protects against privilege escalation through its use of logging and  
1298 monitoring, which enables it to detect unauthorized changes in user attribute information.

- 1299       • Alternatively, an adversary attempting to achieve privilege escalation could use the  
1300       technique of creating an account for a new (nonexistent) user in one of the enterprise's  
1301       directories and giving that new user the desired higher level of privileges.

1302 If such an account is created in a directory directly rather than being provisioned via the  
1303 Policy Administration and Provisioning capabilities, the Security Monitoring capability is  
1304 designed to detect that the account was not created using the converged provisioning  
1305 system and generate an alert.

- 1306       ▪ Credential access results when an adversary obtains access to enterprise resources that he is not  
1307       authorized to access. An adversary employing the tactic of credential access could use the  
1308       technique of trying to obtain legitimate user credentials that belong to another user by  
1309       eavesdropping on these credentials as they are sent to and from directories in the network.

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

### 6.5.5 Deployment Recommendations

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

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

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

#### 6.5.5.2 Other Security Best Practices [6]

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

- 1342       ▪ Segregate reference design capabilities onto their own subnetwork, separate from the  
1343       production network, either physically or by using virtual private networks and port-based  
1344       authentication or similar mechanisms.
- 1345       ▪ Protect the various reference design subnetworks from each other and from the production  
1346       network using security capabilities such as firewalls and intrusion detection devices that are  
1347       configured according to best practices.
- 1348       ▪ Configure firewalls to limit connections between the reference design network and the  
1349       production network, except for connections needed to support required internetwork  
1350       communications to specific IP address and port combinations in certain directions.
- 1351       ▪ Configure and verify firewall configurations to ensure that data transmission to and from  
1352       reference design capabilities is limited to only those interactions that are needed. All  
1353       communications that are permitted should be restricted to specific protocols and IP address and  
1354       port combinations in specific directions.
- 1355       ▪ Monitor the firewalls that separate the various reference design subnetworks from one another.
- 1356       ▪ NIST SP 1800-9C: *How-To Guides* contain the firewall configurations that show the rules that  
1357       were implemented in each of the firewalls for the example implementation. These  
1358       configurations are provided to enable the reader to reproduce the traffic filtering/blocking that  
1359       was achieved in the implementation.
- 1360       ▪ Apply encryption or integrity-checking mechanisms to all information exchanged between  
1361       reference design capabilities (i.e., to all user access, policy, and log information exchanged) so  
1362       that tampering can be detected. Use only encryption and integrity mechanisms that conform to  
1363       most recent industry best practices. Note that in the case of directory reads and writes,  
1364       protected mode is defined as the use of LDAPS (RFC 2830).
- 1365       ▪ Strictly control physical access to both the reference design and the production network.
- 1366       ▪ Deploy a separate, complete system for PAM.
- 1367       ▪ Deploy a configuration management system to serve as a “monitor of monitors” to ensure that  
1368       if any changes are made to the list of information logged and reported to the Monitoring  
1369       Capability or to the analytics in the Monitoring Capability, notifications will be generated. Such a  
1370       system could also serve to monitor whether reference design Monitoring capabilities such as log  
1371       integrity capabilities or the Monitoring Capability itself go offline or stop functioning and  
1372       generate alerts when these capabilities become unresponsive.
- 1373       ▪ Deploy a system that audits and analyzes directory contents to create a description of who has  
1374       access to what resources and validate that these access permissions correctly implement the  
1375       enterprise’s intended business process and access policies.

### 1376   6.5.5.3 *Policy Recommendations*

- 1377       ▪ Define the access policies to enforce the principles of least privilege and separation of duties.

- 1378       ▪ Equip the Monitoring capability with as complete a set of rules as possible to take full advantage  
1379       of the ability to identify anomalous situations that can signal a cyber event. Define enterprise-  
1380       level workflows that include business and security rules to determine each user's access control  
1381       authorizations and ensure that enterprise access control policy is enforced as completely and  
1382       accurately as possible.
- 1383       ▪ Develop an attack model to help determine the types of things that should generate alerts.
- 1384       ▪ Grant only a very few users (e.g., human resource administrators) the authority to modify  
1385       (initiate, change, or delete) employee access information. Require the approval of more than  
1386       one individual to be received to initiate employee access information updates. Log all employee  
1387       access information modifications that are made. Define workflows to enforce these  
1388       requirements.
- 1389       ▪ Grant only a very few users (e.g., access rules administrators) the authority to modify (initiate,  
1390       change, or delete) access rules. Require the approval of more than one individual to be received  
1391       to initiate access rule updates. Log all access rule modifications that are made. Define workflows  
1392       to enforce these requirements.
- 1393       ▪ Grant only a very few users (e.g., security analyst) the authority to modify (initiate, change, or  
1394       delete) the analytics that are applied to log information by the Monitoring capability to  
1395       determine what constitutes an anomaly and generates an alert. Any changes made to the  
1396       analytics should, by policy, require the approval of more than one individual, and these changes  
1397       should themselves be logged, with the logs sent to a monitor-of-monitors system other than the  
1398       Monitoring Capability and to all security analysts and other designated individuals. Define  
1399       workflows to enforce these requirements.
- 1400    *6.5.5.4 Privileged Access Recommendations [7]*
- 1401       ▪ Deploy a separate, complete system for privileged access management.
- 1402       ▪ Limit the number of privileged accounts on reference design capabilities to one or two specific  
1403       console administrators (if the capability is on a physical machine) or virtual administrators (if the  
1404       capability is virtual) and a backup administrator account. Limit the number of persons who serve  
1405       as console administrator for more than one capability.
- 1406       ▪ Require all users logging in to any reference design capability to do so via the PAM (to ensure  
1407       that all privileged user activity is logged and that these logs will be sent to the Monitoring  
1408       capability). Forbid all reference design capabilities from having their consoles accessed directly  
1409       in a way that bypasses the PAM.
- 1410       ▪ Ensure that any administrative changes to the PAM (i.e., the creation of any new privileged user  
1411       accounts, the modification of privileges in privileged user accounts, or a change to the list of  
1412       PAM activity that is logged) require, by policy, the approval of more than two individuals. Also,  
1413       ensure that all administrative changes to the PAM are logged and will generate notifications.

- 1414       ▪ Require the PAM and VE PAM consoles to be accessed in person rather than permitting them to  
1415       be accessed remotely.
- 1416       ▪ Configure the PAM to have an always-on connection to all devices in the reference design so  
1417       that it can monitor each device's console port. This configuration ensures that all activity  
1418       performed over the console port will be logged for monitoring and audit purposes. Configure  
1419       the PAM such that if it's always-on connection to any device is disconnected, an alert is  
1420       generated. This configuration ensures that security auditors can be aware of any times during  
1421       which the console port of a device might have been accessed without the activity being logged  
1422       or monitored.

## 1423   6.6 Security Evaluation Summary

1424   The security benefits of the reference design include:

- 1425       ▪ converged management of user access information and policy
- 1426       ▪ user access information provisioning that is governed by documented and repeatable business  
1427       processes (workflows)
- 1428       ▪ rapid provisioning and de-provisioning using consistent, efficient, and automated processes
- 1429       ▪ centralized log storage to support the ability to apply monitoring and analytics across  
1430       capabilities to detect potential security events, as well as to easily track and audit all user access  
1431       information and policy changes, provisioning requests, and directory modifications.

1432   These convergence, automation, and monitoring capabilities increase the security of organizations that  
1433   adopt the reference design.

1434   Automation of the administration and provisioning of user access information enables efficient, quick,  
1435   and consistent enforcement of the principles of least privilege and separation of duties with respect to  
1436   the access authority granted to each enterprise user. By performing administration and provisioning  
1437   automatically, the reference design eliminates the need for individuals or groups of system  
1438   administrators to manually modify, monitor, or audit the content of each of the enterprise's directories.  
1439   Such automation improves security by reducing the possibility of human error being introduced during  
1440   these processes. It ensures that when users are added or removed, or their responsibilities and the  
1441   things they are authorized to do change, the modifications that need to be made to the user access  
1442   information that determines what systems they have access to, when they have access to them, and  
1443   what they can do on those systems can be provisioned from a single, converged location that  
1444   automatically propagates these changes to all directories throughout the enterprise. These access  
1445   information changes can be provisioned accurately and consistently throughout the enterprise  
1446   instantaneously, ensuring that each employee's access permissions are synchronized across all  
1447   enterprise directories. These capabilities help to reduce the so-called privilege creep that sometimes  
1448   occurs as a user's role changes, and he or she is given access to additional systems without necessarily  
1449   having his or her previous access privileges reduced or modified accordingly. Privilege creep can create



1450 opportunities for insider threat attacks. These capabilities also help to reduce the possibility that a  
1451 user's access permissions become inconsistent across directories.

1452 The reference design also automatically monitors changes to the content of each directory and supports  
1453 an audit system by sending logs from all reference design capability to a single location (the Monitoring  
1454 capability). Consolidation of logs from all reference design capabilities at the Monitoring capability  
1455 enables the reference design to correlate the logs of updates made to each enterprise directory with  
1456 logs from the policy administration and provisioning capabilities and from the VDS in a way that is not  
1457 possible when the logs generated by these capabilities are not consolidated at a single location. This  
1458 consolidation enables the reference design to ensure that access information updates that are made to  
1459 the enterprise's directories are in fact the result of personnel status information modifications input by  
1460 HR, defined and approved according to business workflow rules and access policy, and provisioned via  
1461 the reference design.

1462 Use of the Monitoring capability has the potential to help eliminate access policy inconsistencies that  
1463 could result from human error, as well as to detect security incidents that may be the result of a  
1464 deliberate attack. Log consolidation, combined with the ability to monitor and apply analytics to the logs  
1465 generated by all reference design capabilities, makes it possible for the reference design to  
1466 automatically detect anomalous situations that can indicate a security breach that would be more  
1467 difficult, if not impossible, to detect at any single user access information directory being considered in  
1468 isolation. In addition, although it does not include an audit solution, the reference design enables  
1469 access-related audits to be performed easily and efficiently by aggregating all log information in the  
1470 Monitoring capability.

1471 As with any solution, the reference design introduces new capabilities to the enterprise, and with any  
1472 new capabilities come new threat surfaces. However, these threats can be mitigated using mechanisms  
1473 designed to secure access to the new capabilities and to the user access information and logs that they  
1474 exchange and store. In addition, the reference design's security monitoring and analytics capability also  
1475 helps mitigate threats by systematically subjecting the logs from all reference design capabilities to  
1476 anomaly detection analytics that ensure the authenticity of all directory entries and updates.



## 7 Functional Evaluation

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

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

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

### 7.1 ARM Functional Test Plan

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

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

1501 Table 7-1 Test Case Fields

Test Case Field	Description
<b>Parent requirement</b>	Identifies the top-level requirement or the series of top-level requirements leading to the testable requirement.
<b>Testable requirement</b>	Drives the definition of the remainder of the test case fields. Specifies the capability to be evaluated.
<b>Associated Security Controls</b>	The NIST SP 800-53 Rev. 4 controls addressed by the test case.
<b>Description</b>	Describes the objective of the test case.
<b>Associated test cases</b>	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).
<b>Preconditions</b>	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.
<b>Procedure</b>	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.
<b>Expected results</b>	The expected results for each variation in the test procedure.
<b>Actual results</b>	The observed results.
<b>Overall result</b>	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.

1502 

## 7.2 ARM Use Case Requirements

1503 Table 7.2 identifies the ARM functional evaluation requirements that are addressed in this test plan and  
1504 their associated test cases. The teller application access attribute is held in the OpenLDAP directory and  
1505 the loan application access attribute is held in Active Directory. These applications will be referenced  
1506 throughout the test plans to verify directory modifications. The NCCoE does not have a mainframe  
1507 application that can be used for testing. Therefore, verification of RACF changes will be done manually  
1508 through inspection of the directory contents.

1509 Table 7-2 ARM Functional Requirements

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

Capability Requirement (CR) ID	Parent Requirement	Sub-requirement 1	Sub-requirement 2	Test Case
<b>CR 4</b>	The ARM example implementation shall include a security Monitoring capability that can detect changes to user attributes and group memberships in the following:			
<b>CR 4.a</b>		Active Directory (AD) via logs from:		
<b>CR-4.a.1</b>			AD	ARM-4
<b>CR-4.a.2</b>			Radiant Logic	ARM-4
<b>CR-4.a.3</b>			AlertEnterprise	ARM-4
<b>CR 4.b</b>		OpenLDAP via logs from:		
<b>CR-4.b.1</b>			OpenLDAP	ARM-4
<b>CR-4.b.2</b>			Radiant Logic	ARM-4
<b>CR-4.b.3</b>			AlertEnterprise	ARM-4
<b>CR 4.c</b>		RACF via logs from:		
<b>CR-4.c.1</b>			Vanguard	ARM-4
<b>CR-4.c.2</b>			Radiant Logic	ARM-4
<b>CR-4.c.3</b>			AlertEnterprise	ARM-4
<b>CR 5</b>	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:			
<b>CR 5.a</b>		Active Directory user changes with no correlated log received from:		ARM-5
<b>CR-5.a.1</b>			AD	ARM-5
<b>CR-5.a.2</b>			Radiant Logic	ARM-5
<b>CR-5.a.3</b>			AlertEnterprise	ARM-5
<b>CR 5.b</b>		OpenLDAP user changes with no correlated log received from:		
<b>CR-5.b.1</b>			OpenLDAP	ARM-5
<b>CR-5.b.2</b>			Radiant Logic	ARM-5
<b>CR-5.b.3</b>			AlertEnterprise	ARM-5
<b>CR 5.c</b>		RACF (Vanguard) user changes with no correlated log received from:		
<b>CR-5.c.1</b>			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

1510

1511 **7.3 Test Case: ARM-1**1512 **Table 7-3 Test Case ID: ARM-1**

<b>Parent requirement</b>	(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.
<b>Testable requirement</b>	(CR 1.a) Active Directory, (CR 1.b) OpenLDAP, (CR 1.c) RACF
<b>Description</b>	Show that the ARM example implementation can create users in the various directories with the appropriate access and permissions.
<b>Associated test cases</b>	N/A
<b>Associated CSF Subcategories</b>	PR.AC-1, PR.AC-4
<b>Preconditions</b>	<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>
<b>Procedure</b>	<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>
<b>Expected Results (pass)</b>	<p>Access Allowed (CR 1.a-c)</p> <p>Users with allowed access can log in to loan and teller demo applications.</p> <p>Access Denied (CR 1.a-c)</p> <p>Users without allowed access are unable to log in to loan and teller demo applications.</p>
<b>Actual Results</b>	<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>
<b>Overall Result</b>	<p>Pass/Fail (with comments)</p>

1513



1514 **7.4 Test Case ARM-2**1515 **Table 7-4 Test Case ID: ARM-2**

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

---

(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)
----------------	---------------------------

1516

1517 **7.5 Test Case ARM-3**1518 **Table 7-5 Test Case ID: ARM-3**

<b>Parent requirement</b>	(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.
<b>Testable requirement</b>	(CR 3.a) Active Directory, (CR 3.b) OpenLDAP, (CR 3.c) RACF
<b>Description</b>	Show that the ARM solution can change user attributes and group memberships within directories.
<b>Associated test cases</b>	CR 1
<b>Associated CSF Subcategories</b>	PR.AC-1, PR.AC-4
<b>Preconditions</b>	<p>Reuse ARM example implementation in the state after ARM-1 is completed.</p> <p>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.</p>
<b>Procedure</b>	<p>Operate the example implementation to read the new HR file.</p> <p>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.</p> <p>Use the ARM workflow to deny access for the set of users with known access chosen in 1 above.</p> <p>Use the ARM workflow to allow access for the set of users known to not have access chosen in 1 above.</p> <p>Process the HR dataset with the AlertEnterprise system.</p> <p>Verify that the AlertEnterprise successfully processes the dataset.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.
<b>Expected Results (pass)</b>	<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:</p> <p>(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.</p> <p>(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.</p> <p>(CR 3.c) RACF: User accesses are changed as expected.</p>
<b>Actual Results</b>	<p>This system functioned appropriately and provided the expected results.</p> <p>(CR 3) The ARM example implementation can change user attributes and group memberships in the following directories:</p> <p>(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.</p> <p>(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.</p> <p>(CR 3.c) RACF: User accesses changed as expected.</p>
<b>Overall Result</b>	Pass/Fail (with comments)

## 7.6 Test Case ARM-4

Table 7-6 Test Case ID: ARM-4

<b>Parent requirement</b>	(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:
<b>Testable requirement</b>	(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
<b>Description</b>	Show that the ARM solution can detect when user changes occur within the directories.
<b>Associated test cases</b>	CR 1
<b>Associated CSF Subcategories</b>	DE.AE-1, DE.AE-3, DE.AE-5
<b>Preconditions</b>	Reuse ARM example implementation in the state after ARM-1 is completed.
<b>Procedure</b>	<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>
<b>Expected Results (pass)</b>	<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>

	(CR 4.c) RACF (Vanguard) from (CR-4.c.1) Vanguard, (CR-4.c.2) Radiant Logic, (CR-4.c.3) AlertEnterprise
<b>Actual Results</b>	<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>
<b>Overall Result</b>	Pass/Fail (with comments)

1522

1523 **7.7 Test Case ARM-5**1524 **Table 7-7 Test Case ID: ARM-5**

<b>Parent requirement</b>	(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:
<b>Testable requirement</b>	<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>
<b>Description</b>	Show that the ARM example implementation can detect when anomalous user changes occur within the directories.
<b>Associated test cases</b>	CR 1
<b>Associated CSF Subcategories</b>	DE.AE-3, DE.AE-5
<b>Preconditions</b>	Reuse ARM example implementation in the state after ARM-1 is completed.
<b>Procedure</b>	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.
<b>Expected Results (pass)</b>	<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:</p> <p>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>

<b>Actual Results</b>	<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>
<b>Overall Result</b>	Pass/Fail (with comments)

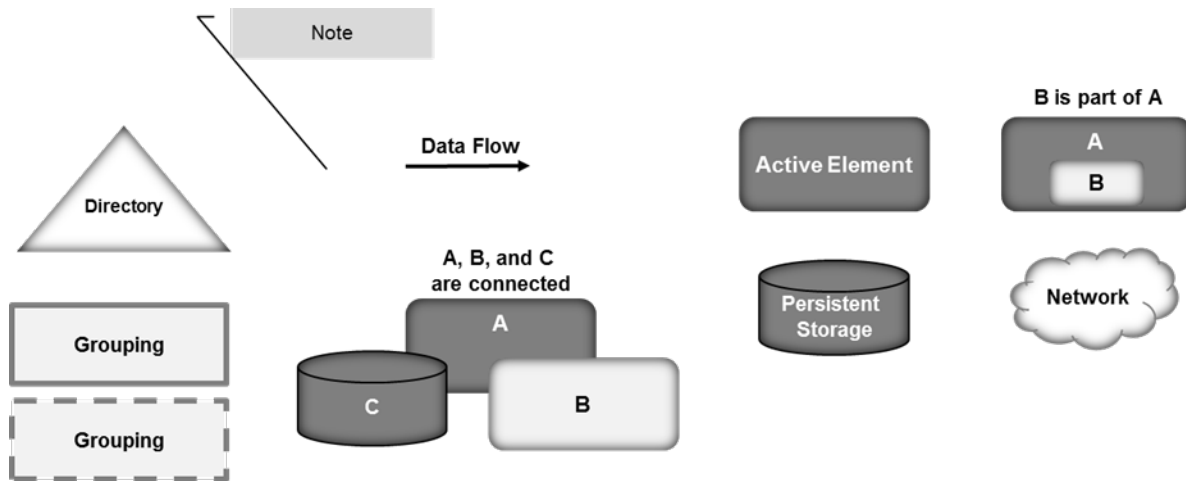


## 1525 **Appendix A List of Acronyms**

1526	<b>AD</b>	Active Directory
1527	<b>ARM</b>	Access Rights Management
1528	<b>CAT</b>	Cybersecurity Assessment Tool
1529	<b>CR</b>	Capability Requirement
1530	<b>CSF</b>	Cybersecurity Framework
1531	<b>.csv</b>	Comma-Separated Value
1532	<b>DNS</b>	Domain Name Service
1533	<b>FFIEC</b>	Federal Financial Institutions Examination Council
1534	<b>FS-ISAC</b>	Financial Sector Information Sharing and Analysis Center
1535	<b>HR</b>	Human Resources
1536	<b>ID</b>	Identity
1537	<b>IP</b>	Internet Protocol
1538	<b>LDAPS</b>	Lightweight Directory Access Protocol Secure
1539	<b>NCCoE</b>	National Cybersecurity Center of Excellence
1540	<b>NIST</b>	National Institute of Standards and Technology
1541	<b>OS</b>	Operating System
1542	<b>PAM</b>	Privileged Account Management
1543	<b>RACF</b>	Resource Access Control Facility
1544	<b>RMF</b>	Risk Management Framework
1545	<b>SIM</b>	Security Information Management
1546	<b>TLS</b>	Transport Layer Security
1547	<b>VE</b>	Virtual Environment
1548	<b>VDS</b>	Virtual Directory System
1549	<b>VLAN</b>	Virtual Local Area Network
1550	<b>VM</b>	Virtual Machine

1551 **Appendix B Legend for Diagrams**

1552



## 1553 Appendix C References

1554

- [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>

## DISCLAIMER

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

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

## FEEDBACK

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

Comments on this publication may be submitted to: [financial\\_nccoe@nist.gov](mailto:financial_nccoe@nist.gov)

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

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

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

## NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

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

## NIST CYBERSECURITY PRACTICE GUIDES

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

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

## ABSTRACT

Managing access to resources (data) is complicated because internal systems multiply and acquisitions add to the complexity of an organization's IT infrastructure. Identity and access management (IdAM) is the set of technology, policies, and processes that are used to manage access to resources. Access rights management (ARM) is the subset of those technologies, policies, and processes that manage the rights of individuals and systems to access resources (data). In other words, an ARM system enables a company to give the right person the right access to the right resources at the right time. The goal of this project is to demonstrate an ARM solution that is a standards-based technical approach to coordinating and automating updates to and improving the security of the repositories (directories) that maintain the user access information across an organization. The coordination improves cybersecurity by ensuring that user access information is updated accurately (according to access policies), including disabling accounts or revoking access privileges as user resource access needs change. Cybersecurity is also improved through better monitoring for unauthorized changes (e.g., privilege escalation). The system executes user access changes across the enterprise according to corporate access policies quickly, simultaneously, and consistently. The ARM reference design and example implementation are described in this NIST Cybersecurity "Access Rights Management" practice guide. This project resulted from discussions among NCCoE staff and members of the financial services sector.

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

## KEYWORDS

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

## ACKNOWLEDGMENTS

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

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

The technology vendors who participated in this build submitted their capabilities in response to a notice in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. We worked with:

Product Vendor	Component Name	Function
<a href="#">AlertEnterprise</a>	Enterprise Guardian	Access policy management, administration and account provisioning system

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



## Contents

<b>1</b>	<b>Introduction .....</b>	<b>1</b>
1.1	Practice Guide Structure .....	1
1.2	Build Overview .....	2
1.3	Typographical Conventions .....	2
1.4	Logical Architecture Summary .....	3
1.5	Network Diagrams .....	4
1.6	NCCoE Lab .....	4
<b>2</b>	<b>Product Installation Guides .....</b>	<b>7</b>
2.1	AlertEnterprise .....	7
2.1.1	How It's Used .....	7
2.1.2	Virtual Machine Configuration.....	7
2.1.3	Prerequisites .....	8
2.1.4	Java .....	8
2.1.5	Apache Activemq .....	8
2.1.6	Oracle DB .....	9
2.1.7	7-Zip.....	9
2.1.8	Installation .....	9
2.1.9	Install and Configure Tomcat.....	10
2.1.10	Configure the Database Server .....	10
2.1.11	Deploying the Application .....	11
2.1.12	Start the Server .....	12
2.1.13	Provisioning Configuration .....	12
2.1.14	Creating System Connectors.....	12
2.1.15	User Data Source.....	15
2.1.16	Process Designer .....	15
2.1.17	Policies.....	15
2.1.18	Rules .....	16
2.1.19	Policy Designer.....	16
2.1.20	Triggers Field Map.....	18
2.1.21	Form Customization .....	19

97	2.1.22	User Field Mapping .....	19
98	2.1.23	Provisioning Mapping.....	20
99	2.1.24	External Provisioning Attributes .....	22
100	2.1.25	Role Repository .....	22
101	2.1.26	Enabling SSL .....	24
102	2.2	HyTrust Cloud Control.....	24
103	2.2.1	How Its Used.....	24
104	2.2.2	Virtual Machine Configuration.....	25
105	2.2.3	Installing Vcenter Server.....	25
106	2.2.4	Configuring Vcenter Server.....	26
107	2.2.5	Deploying HTCC.....	26
108	2.2.6	Configuring HTCC .....	26
109	2.2.7	Integrating With Active Directory .....	30
110	2.2.8	Creating and Deploying Access Policies.....	32
111	2.2.9	Configure Logging .....	34
112	2.3	Microsoft Active Directory .....	35
113	2.3.1	How It's Used .....	35
114	2.3.2	Virtual Machine Configuration.....	35
115	2.3.3	Installing AD.....	35
116	2.3.4	DNS Configuration.....	36
117	2.3.5	Installing Splunk Universal Forwarder.....	36
118	2.3.6	Install Security Compliance Manager.....	37
119	2.3.7	Group Policy Object (GPO) Configuration .....	37
120	2.3.8	Script: AddOnlineStatus.ps1.....	45
121	2.3.9	LDAPS Configuration .....	46
122	2.4	NextLabs Entitlement Manager.....	48
123	2.4.1	How It's Used .....	48
124	2.4.2	Virtual Machine Configuration.....	48
125	2.4.3	Prerequisites .....	49
126	2.4.4	Installing NextLabs .....	49
127	2.5	OpenLDAP .....	66
128	2.5.1	How It's Used .....	66

129	2.5.2	Virtual Machine Configuration.....	66
130	2.5.3	Firewall Configuration .....	67
131	2.5.4	Installation .....	67
132	2.5.5	Audit Configuration .....	68
133	2.5.6	STARTTLS and LDAPS Configuration.....	69
134	2.5.7	Formatting Audit Logs .....	71
135	2.5.8	Script: /etc/ldap/logs/auditlogscript.....	71
136	2.5.9	Script: /etc/ldap/logs/add-timestamp.py.....	71
137	2.5.10	Script: /etc/cron.daily/openldap-status .....	72
138	2.6	Radiant Logic .....	72
139	2.6.1	How Its Used.....	73
140	2.6.2	Virtual Machine Configuration.....	73
141	2.6.3	Installing the Virtual Directory .....	73
142	2.6.4	Configuring VD .....	73
143	2.6.5	Configure Logging .....	78
144	2.6.6	Configure Views for SharePoint .....	82
145	2.6.7	Scripts .....	88
146	2.6.8	Script: RadiantOnlineStatus.ps1 .....	89
147	2.6.9	Script: VanguardOnlineStatus.ps1 .....	90
148	2.6.10	LDAPS Configuration .....	91
149	2.7	SharePoint .....	91
150	2.7.1	How It's Used .....	91
151	2.7.2	Virtual Machine Configuration.....	91
152	2.7.3	Prerequisites .....	91
153	2.7.4	Installing SharePoint 2013 .....	91
154	2.7.5	Configuring SharePoint.....	92
155	2.7.6	Web Configs.....	94
156	2.8	Splunk.....	98
157	2.8.1	How It's Used .....	98
158	2.8.2	Installation .....	99
159	2.8.3	Queries .....	99
160	2.8.4	Query: Detect User Provisioning Accounts Events.....	99

161	2.8.5	Query: Authorized and Unauthorized Provisioning Trend Line Chart.....	100
162	2.8.6	Query: Combined Provisioning Trend Line Chart.....	101
163	2.8.7	Query: Detect modifications to High Value or Privileged Accounts.....	102
164	2.8.8	Query: Virtual Directory Server Offline Detection .....	103
165	2.8.9	Query: Critical Servers Offline.....	103
166	2.8.10	SSL Forwarding.....	103
167	2.9	TDI ConsoleWorks.....	104
168	2.9.1	How It's Used .....	104
169	2.9.2	Virtual Machine Configuration.....	104
170	2.9.3	Firewall Configuration .....	104
171	2.9.4	Installation .....	105
172	2.9.5	Console Connection Configuration .....	105
173	2.9.6	Graphical Gateway Configuration.....	105
174	2.9.7	Graphical Connection Configuration.....	106
175	2.9.8	Profile Creation .....	106
176	2.9.9	Access Controls .....	107
177	2.9.10	pUser Auditing .....	113
178	2.9.11	Cron Configuration: /etc/crontab .....	113
179	2.9.12	Scripts: connectionreporting .....	113
180	2.9.13	Scripts: bashconnectionreporting.....	114
181	2.10	Network Firewall Configuration .....	114
182	2.10.1	Firewall Configuration for Backbone Subnet.....	114
183	2.10.2	Firewall Configuration for Common Services Subnet .....	164
184	2.10.3	Firewall Configuration for ID-ARM Subnet.....	192
185	2.10.4	Firewall Configuration for Private Cloud Subnet .....	222
186	2.10.5	Firewall Configuration for the Management and Monitoring Subnet .....	239
187	<b>Appendix A</b>	<b>List of Acronyms .....</b>	<b>267</b>
188			

189    **List of Tables**

190    Table 1-1 NCCoE Lab Network and System IP Addresses ..... 6

191    **List of Figures**

192    Figure 1-1 Logical Access Rights Management Lab Build Architecture ..... 3

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

194    Figure 1-3 NCCoE Lab Networking Diagram ..... 5

195    Figure 1-4 NCCoE Lab Networking Diagram ..... 6

# 1 Introduction

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

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

## 1.1 Practice Guide Structure

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

The guide contains three volumes:

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

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

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

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

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

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

**IT professionals** who want to implement an approach like this will find the whole Practice Guide useful. The guide's information will provide insight into the resources and skills needed to implement an ARM solution. You can use the How-To portion of the guide, NIST SP 1800-9c (which is this document), to replicate all or parts of the example implementation created in our lab. *NIST SP 1800-9c* provides specific product installation, configuration, and integration instructions for implementing the example implementation. We do not re-create the product manufacturers' documentation, which is generally widely available. Rather, we show how we incorporated the products in our environment to create an example implementation.

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

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

## 1.2 Build Overview

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

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

## 1.3 Typographical Conventions

The following table presents typographic conventions used in this volume.

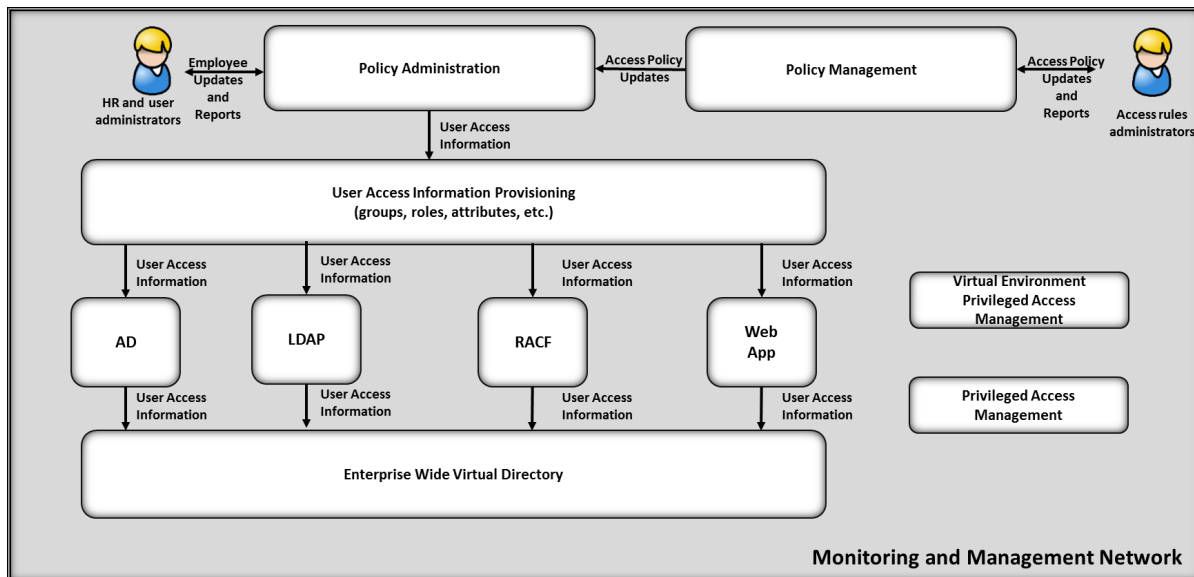
Typeface/ Symbol	Meaning	Example
<i>Italics</i>	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the <i>NCCoE Glossary</i> .
<b>Bold</b>	names of menus, options, command buttons and fields	Choose <b>File &gt; Edit</b> .
Monospace	command-line input, on- screen computer output,	<code>mkdir</code>

Typeface/ Symbol	Meaning	Example
	sample code examples, status codes	
<b>Monospace Bold</b>	command-line user input contrasted with computer output	<code>service sshd start</code>
<a href="#">blue text</a>	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at <a href="http://nccoe.nist.gov">http://nccoe.nist.gov</a>

## 1.4 Logical Architecture Summary

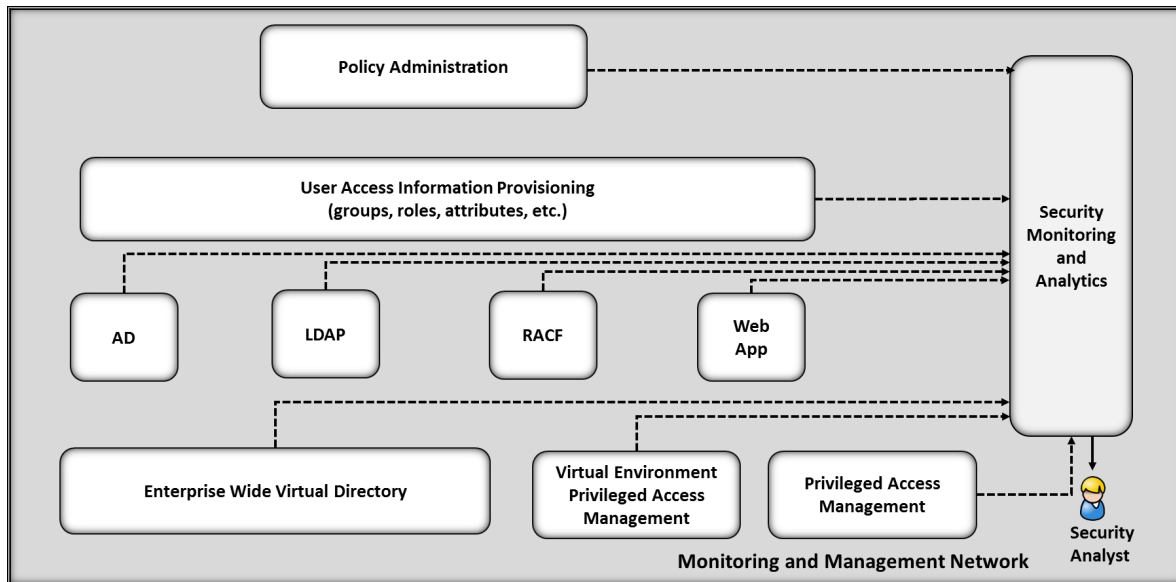
NIST Special Publication 1800-9b (SP1800-9b) describes an example implementation consisting of user access management (including provisioning) and security monitoring / data collection. SP1800-9b includes a much more detailed description of the architecture for building an instance of the example implementation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

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





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



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

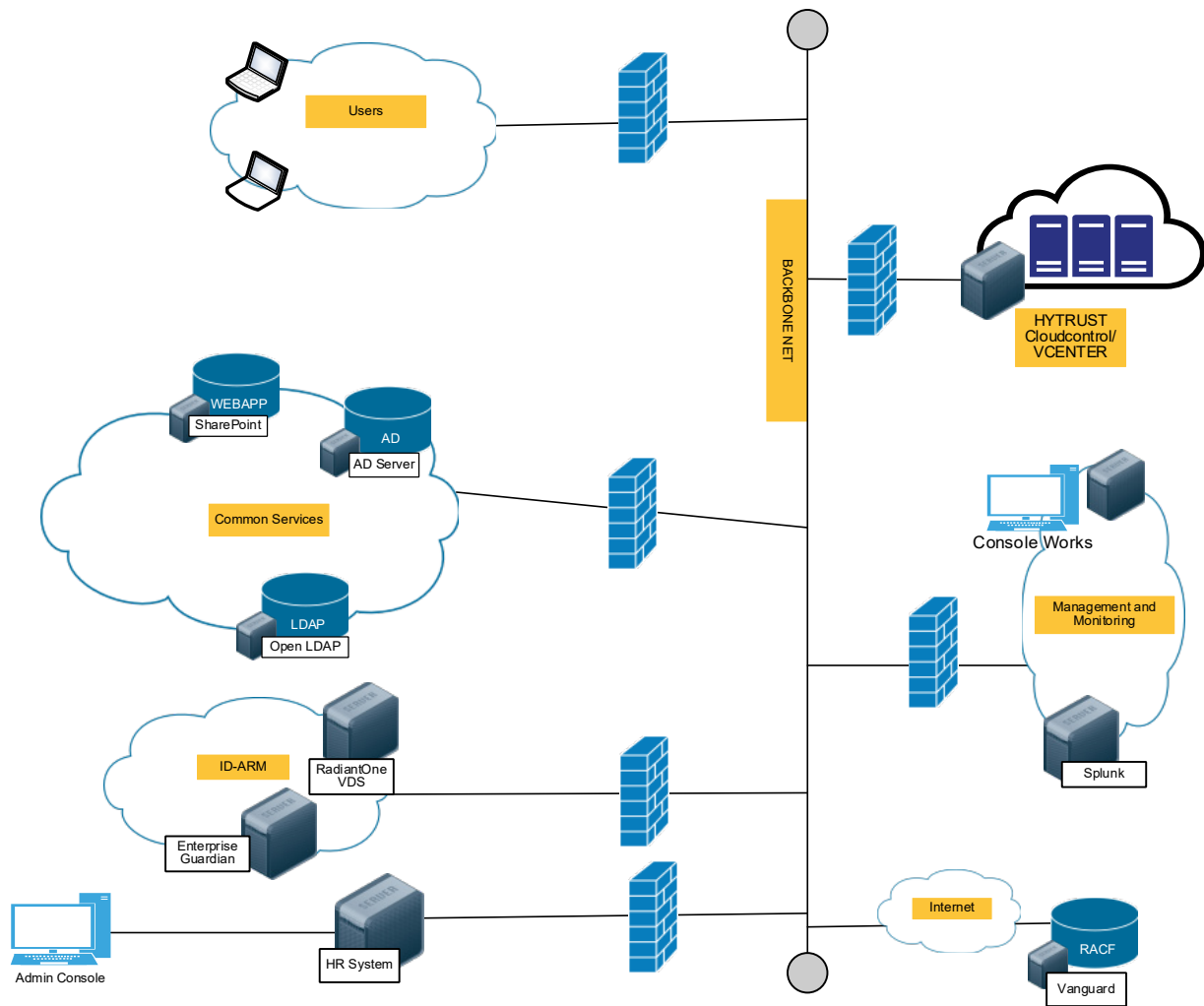
## 274 1.5 Network Diagrams

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

## 278 1.6 NCCoE Lab

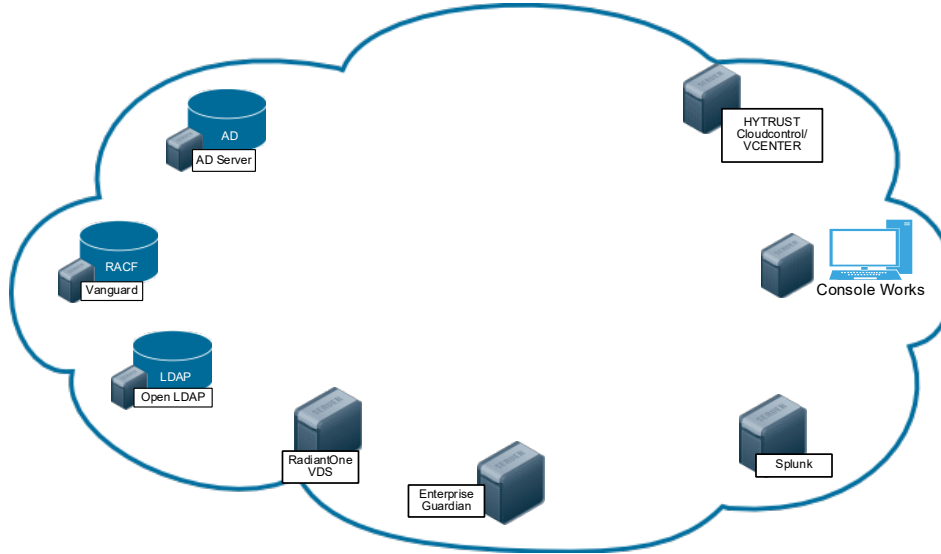
279 Figures 1-3 and Figure 1-4 show the network configurations used in the example implementation.

280 Figure 1-3 NCCoE Lab Networking Diagram



281

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



283  
 284 The following table includes the IP addresses for each of the networks depicted in Figure 1-3 and Figure  
 285 1-4.

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

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

## 2 Product Installation Guides

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

### 2.1 AlertEnterprise

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

#### 2.1.1 How It's Used

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

#### 2.1.2 Virtual Machine Configuration

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

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

#### Network Configuration (Interface 1)

IPv4 Manual  
IPv6 Disabled  
IP Address: 192.168.14.113  
Netmask: 255.255.255.0  
Gateway: 192.168.14.1  
DNS Name Servers: 192.168.19.10  
DNS-Search Domains: acmefinancial.com

#### Network Configuration (Interface 2)

IPv4 Manual  
IPv6 Disabled  
IP Address: 192.168.17.114  
Netmask: 255.255.255.0  
Gateway: 192.168.17.1  
DNS Name Servers: 192.168.19.10  
DNS-Search Domains: acmefinancial.com

### 2.1.3 Prerequisites

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

Prerequisite software used in this build:

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

### 2.1.4 Java

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

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

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

4. Setting Path:  
PATH= C:\Program Files\Java\JDK1.6.0-21\bin;%PATH%

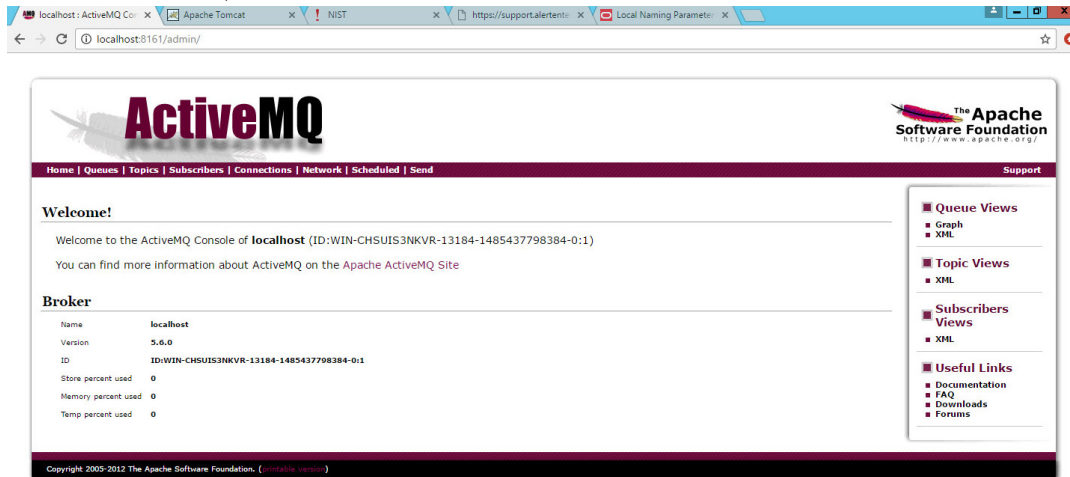
5. Checking JAVA\_HOME and PATH:

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

### 2.1.5 Apache Activemq

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

353 installed>:8161/admin



354

## 355 2.1.6 Oracle DB

- 356 1. Install the Oracle SQL database according to documentation found on the Oracle [website](#).
- 357 2. Ensure the pdborcl pluggable database service name is added correctly in the tnsnames.ora file
- 358 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))

ORACL_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)
    )
  )
```

359

- 360 3. Open a command prompt and test by connecting with this command: **sqlplus**
- 361 **sys/<password>@pdborcl as sysdba.**

## 362 2.1.7 7-Zip

- 363 1. Download and install 7-Zip from [www.7-zip.org](#).

## 364 2.1.8 Installation

365 You can install the AlertEnterprise Enterprise Guardian Application in three steps. This information is

366 also found within the *AlertEnterprise Installation Guide*.

- 367 1. Install and Configure the Apache Tomcat Server.
- 368 2. Configure the database server.

3. Deploy the application.

### 2.1.9 Install and Configure Tomcat

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

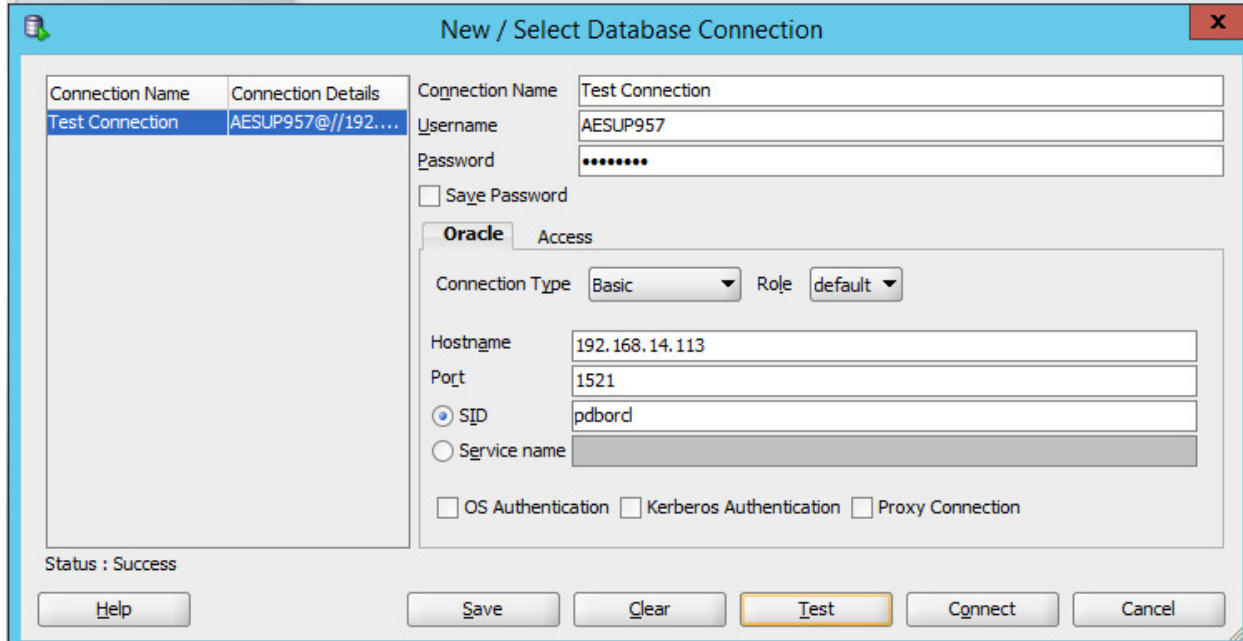
```
-XX:PermSize=1024
-Xms2048m
-Xmx2048m
-Dcom.alnt.fabric.loadInitData=force
"                                "--Dalert.db.update=update
```
4. Click **Apply** and **OK** to close the dialog box.

### 2.1.10 Configure the Database Server

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

1. Create a new schema/SID per your naming convention: **create user <user/schema name> identified by <password>**, you may have to unlock the schema: **alter user <user/schema name> identified by <password> unlock**
2. Use **grant <attribute> to <user/schema name>**; to grant the new user all of the following attributes:  
connect; resource; create synonym; create session; create sequence; create view; unlimited tablespace; create procedure; create trigger; create table

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



### 2.1.11 Deploying the Application

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

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

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



For ORACLE:

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

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

## 2.1.12 Start the Server

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

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

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

## 2.1.13 Provisioning Configuration

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

## 2.1.14 Creating System Connectors

1. Navigate to **Setup > Manual Configuration > Systems > System**.
2. Click **New** to create a new system.
3. Enter the following Definition:
  - a. System Type – Active Directory
  - b. Connector Name – AD
  - c. Connector Description – AD
  - d. Connector Long Description – AD
  - e. Connector Type – LDAP (default)
4. Click **Next**.
5. Enter the following Parameters:
  - a. HostName – 192.168.19.10
  - b. Port Number – 636 (use 389 if SSL is not configured yet)
  - c. Service user Dn – CN=AlertServiceAccount,CN=Users,DC=Acmefinancial,DC=com
  - d. Password – Fsarm@nccoe1
  - e. Use SSL – true (use false if SSL is not configured yet)

- 469 f. User Base DN – OU=Operations,DC=Acmefinancial,DC=com
- 470 g. Group Base DN – DC=Acmefinancial,DC=com
- 471 h. Object Class – user
- 472 i. Is Primary – Yes
- 473 j. LastModified Column role – whenChanged
- 474 k. Last Modified User Column – whenChanged
- 475 6. Click **Next**.
- 476 7. Enter the following parameters:
  - 477 a. Application – AlertAccess
  - 478 b. Check the following boxes – Provisioning, Role Management, Offline System,
  - 479 Allow Modify Role
  - 480 c. Category – production
  - 481 d. Time Zone – Eastern Standard Time
- 482 8. Click **Next**.
- 483 9. Click **Save**.
- 484 10. Repeat Steps 1–9 to add the OpenLDAP and RACF connectors with the following parameters:
  - 485 OpenLDAP:
    - 486 a. System Type – OpenLDAP Server
    - 487 b. Connector Name – OPENLDAP
    - 488 c. Connector Description – OpenLDAP
    - 489 d. Connector Type – OpenLDAP
    - 490 e. HostName – 192.168.19.11
    - 491 f. Port Number – 636 (use 389 if SSL is not configured yet)
    - 492 g. Service user Dn – CN=Admin,DC=Acmefinancial,DC=com
    - 493 h. Password – Fsarm@nccoe1
    - 494 i. Use SSL – true (use false if SSL is not configured yet)
    - 495 j. User Base DN – OU=Operations,DC=Acmefinancial,DC=com
    - 496 k. Group Base DN – OU=Operations,DC=Acmefinancial,DC=com
    - 497 l. Object Class – inetOrgPerson
    - 498 m. Group Object Class Name – groupOfUniqueNames
    - 499 n. Primary Connection – Yes
    - 500 o. LastModified Column role – whenChanged
    - 501 p. Last Modified User Column – whenChanged
    - 502 q. Member Attribute Name for Group – uniqueMember
    - 503 r. LDAP DnName – cn
    - 504 s. LDAP Account Control Column Name – cn
    - 505 t. User Password attributed – default
    - 506 u. Encode Password Required? – default
    - 507 v. LDAP Group Search Attributed – cn
    - 508 w. userIdColumnName (Optional Parameter) – cn
    - 509 x. Application – AlertAccess
    - 510 y. Check the following boxes – Provisioning, Role Management, Offline System,
    - 511 Allow Modify Role
    - 512 z. Category – production
    - 513 aa. Time Zone – Eastern Standard Time
  - 514 RACF:
    - 515 a. System Type – OpenLDAP Server
    - 516 b. Connector Name – RACF\_OPENLDAP

- c. Connector Description – RACF\_OpenLDAP
  - d. Connector Type – OpenLDAP
  - e. HostName – 172.17.212.10
  - f. Port Number – 636 (use 389 if SSL is not configured yet)
  - g. Service user Dn – racfid=TSNI00,profiletype=user,sysplex=sysplex1
  - h. Password – Fsarm@nccoe1
  - i. Use SSL – true (use false if SSL is not configured yet)
  - j. User Base DN – profiletype=user,sysplex=sysplex1
  - k. Group Base DN – profiletype=user,sysplex=sysplex1
  - l. Object Class – racfUser
  - m. Primay Connection – Yes
  - n. LDAP DnName – racfid
  - o. LDAP UserID Column Name – racfid
  - p. User Password attributed – default
  - q. Encode Password Required? – default
  - r. Ignore user check – Yes
  - s. isObjectClassExist – No
  - t. userIdColumnName (Optional Parameter) – racfid
  - u. isCnAttrExists (Optional Parameter) – No
  - v. Application – AlertAccess
  - w. Check the following boxes – Provisioning, Role Management, Offline System, Allow Modify Role
  - x. Time Zone – Eastern Standard Time
- File Connector
- a. System Type – File Connector
  - b. Connector Name – FILE CONNECTOR
  - c. Connector Type – FileConnector
  - d. User Folder Path – C:\Program Files\User
  - e. Role Folder Path – C:\Program Files\Role
  - f. User role Folder Path – C:\Program Files\UserRole
  - g. Column Header for User ID – UserId
  - h. Skip Provisioning – Yes
  - i. Application – AlertAccess
  - j. Check the following boxes – Provisioning, Role Management
  - k. Category – Production
  - l. Time Zone – Eastern Standard Time
- Identity Store
- a. System Type – Database (JDBC J2EE)
  - b. Connector Name – IDENTITYSTORE
  - c. Connector Type – Database (JDBC J2EE)
  - d. User Name – admin
  - e. Password – System@123
  - f. JNDI Name – java:comp/env/jdbc/alntdb
  - g. Application – Alert Access
  - h. Check the following boxes – Provisioning, Role Manangement, Offline System, Identity Provider
  - i. Category – Production
  - j. Time Zone – Eastern Standard Time

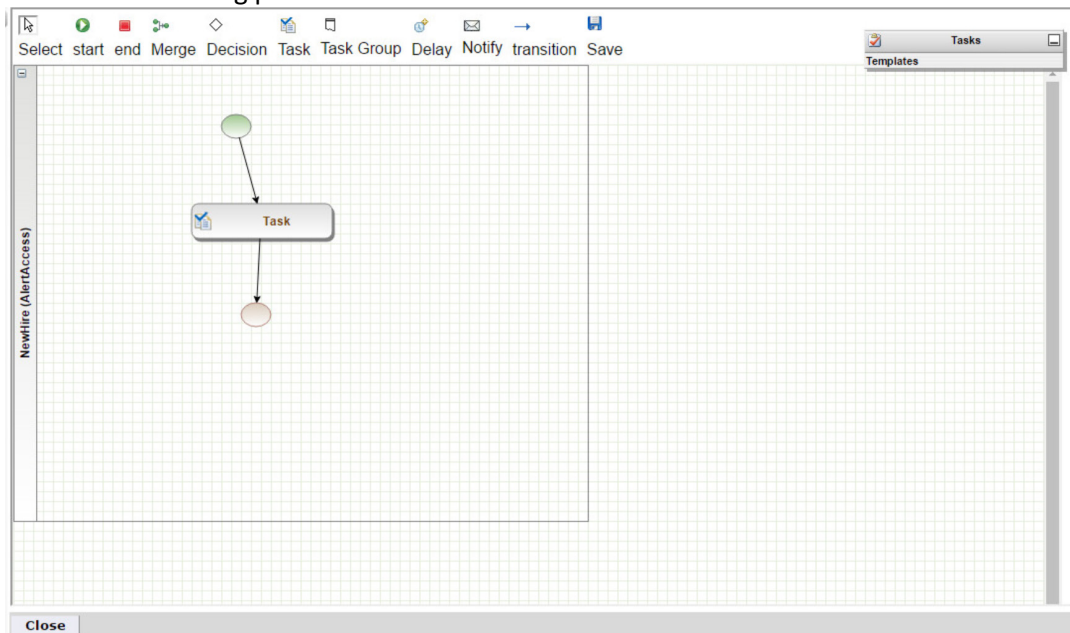
### 2.1.15 User Data Source

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

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

### 2.1.16 Process Designer

1. Navigate to **Setup>Manual Configuration>Process Engine>Process Designer**.
2. Click **New**.
3. Enter **New Hire** as Process Name and **Alert Access** as Rule Type. Click **Next**.
4. Create the following process:



### 2.1.17 Policies

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

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

## 2.1.18 Rules

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

Rule Name	Entity Type	Rule Type	Description	Applicable To	Attributes	Condition
Survey Rule	Workflow	Survey	Survey Rule	Initiator	AND	
NewHire	Workflow	AlertAccess	NewHire	Initiator	AND Request Category	= Change Access
NewHireSuggestDefault	Workflow	AlertAccess	NewHireDefault	Suggest/Default	AND Request Category	1) =NewHire 2) =Change-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

### 2.1.18.1 Suggest/Default Access

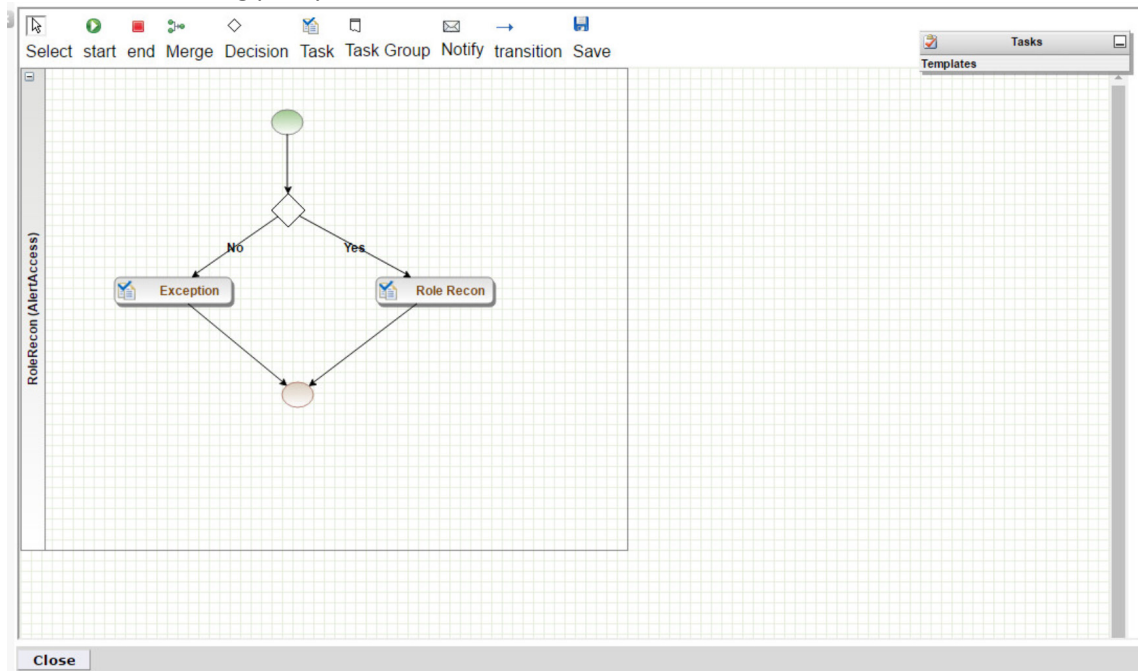
1. Navigate to **Setup>Manual Configuration>Policy Engine>Suggest/Default Access**.
2. Click **New**. Create the following criteria:

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

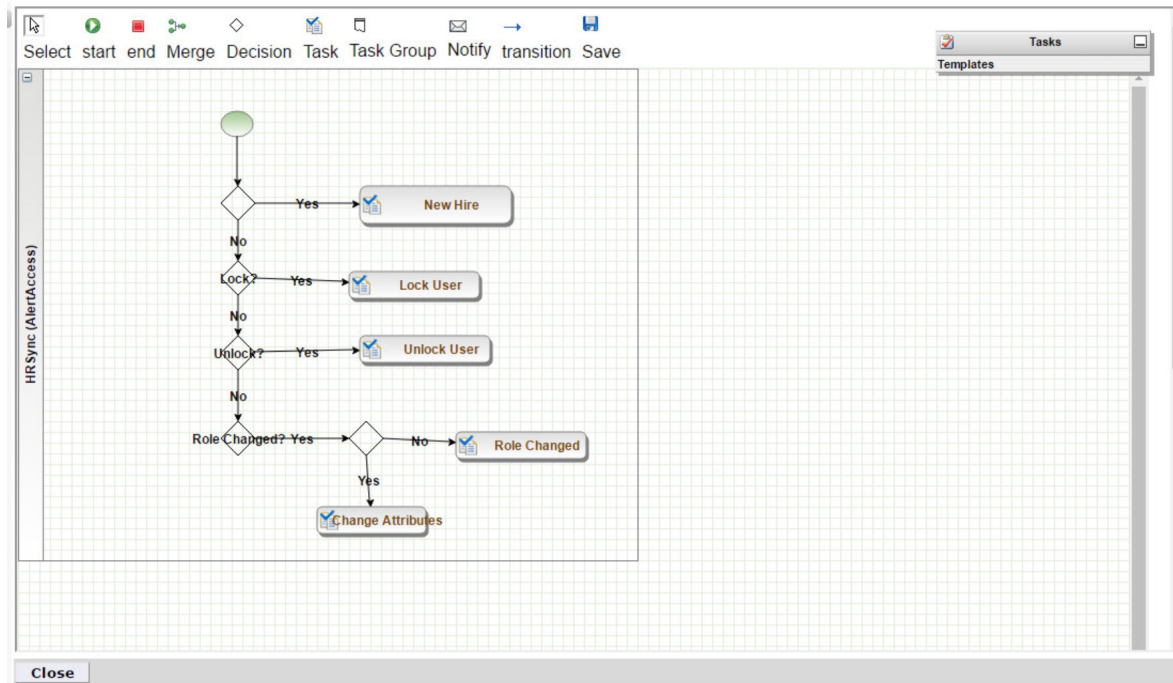
## 2.1.19 Policy Designer

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

588 4. Create the following policy:



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



### 592 2.1.19.1 Rule Action Handlers

- 593 1. Navigate to **Setup>Manual Configuration>Policy Engine>Rule Action Handler**.
- 594 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

### 2.1.19.2 Job Triggers

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

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

### 2.1.20 Triggers Field Map



- 599 1. Navigate to **Setup>Manual Configuration>Job Scheduler>Triggers Field Map**.  
 600 2. Click **Create**. Create the following field map group:  
 601

Group Name	Type
HR Sync	Reconciliation

### 602 2.1.21 Form Customization

- 603 1. Navigate to **Setup>Manual Configuration>Form Customization>Attributes**.  
 604 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
Racprogrammername	Custom	No	No	String	Textbox	Provisioning
Racworkattrusername	Custom	No	No	String	Textbox	Provisioning
Racaddressline1	Custom	No	No	String	Textbox	Provisioning
Racaddressline4	Custom	No	No	String	Texbox	Provisioning

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

### 606 2.1.22 User Field Mapping

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

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



Alias	No	No	6
Email	No	No	7
ManagerId	No	No	8
Department	No	No	9
JobTitle	No	No	10
CompanyName	No	No	11
ManagerName	No	No	12
FullName	No	No	13
Mobile	No	No	14
User Base Dn	No	No	15
ADUserId	No	No	16
LDAPUserId	No	No	17
ADuserName	No	No	18
LDAPuserName	No	No	19
EmployeeNo	No	No	20
Initials	No	No	21
Pager	No	No	22
L	No	No	23
Racfid	No	No	24
Racfprogrammername	No	No	25
Racfworattrusername	No	No	26
Racfaddressline1	No	No	27
Racfaddressline4	No	No	28

### 2.1.23 Provisioning Mapping

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

#### IDENTITYSTORE

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

#### OPENLDAP

Database Attribute Name	Mandatory	AlertEnterprise Attribute Name	Default Value	Editable	Visible	Validation Flag	isUser-Id attribute
<b>Cn</b>	No	LDAPUserId		Yes	Yes	No	Yes
<b>Sn</b>	No	LastName		Yes	Yes	No	No

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

## 617 AD

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

## 618 RACF\_OPENLDAP

Directory Attribute Name	Mandatory	AlertEnterprise Attribute Name	Default Value	Editable	Visible	Validation Flag	isUser-Id attribute
<b>Racfid</b>	Yes	Racfid		No	No	No	Yes
<b>Racworkattruser name</b>	No	Racworkattruser name		No	No	No	No
<b>UserBaseDn</b>	Yes	homeDirectory	profiletype=user,	No	No	No	No

			sysplex=sysplex1				
<b>objectClass</b>	No	UserObjectClass	racfUser	No	No	No	No
<b>Racfprogrammerna</b> <b>me</b>	No	Racfprogrammerna		No	No	No	No
<b>Racfaddressline1</b>	No	Racfaddressline1		No	No	No	No
<b>Racfaddressline4</b>	No	Racfaddressline4		No	No	No	No

## 2.1.24 External Provisioning Attributes

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

### OPENLDAP

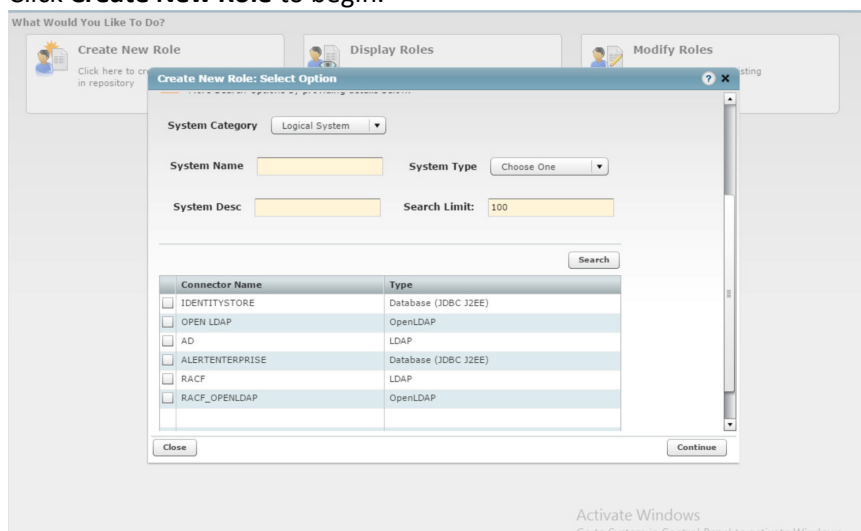
Name	Description
<b>loginShell</b>	loginShell

### RACF\_OPENLDAP

Name	Description
<b>Racfid</b>	Racfid
<b>Racfworkattrusername</b>	Racfworkattrusername
<b>UserBaseDn</b>	UserBaseDn
<b>objectClass</b>	objectClass
<b>Racfprogrammerna</b> <b>me</b>	Racfprogrammerna
<b>Racfaddressline1</b>	Racfaddressline1
<b>Racfaddressline4</b>	Racfaddressline4

## 2.1.25 Role Repository

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



3. Select **Create New Role** from Start.
4. Click **Search** to load the connector names. Select the **OpenLDAP** and **AD** connectors.
5. Click **Continue**.
6. Enter a **Role Name** and **Alias**. They must be identical.

**Create New Resource Role**

Follow the steps below to create Resource Role

**Mandatory fields**

**Details**

Role Name:

Description:

Resource Type: LDAP/OpenLDAP

Resource(s):

[Edit Resources](#)

**Steps**

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

[Previous Step](#) [Next Step](#)

**1 Attributes**

Role Comments Ma...

Role Hex Code:

\* Alias:

Criticality:

Long Description:

Team Rooms:

Functional Area:

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](#)

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

8. Create the following roles in the repository:

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

<b>Teller</b>	AD, OpenLDAP
<b>VM Admin</b>	AD, OpenLDAP

## 2.1.26 Enabling SSL

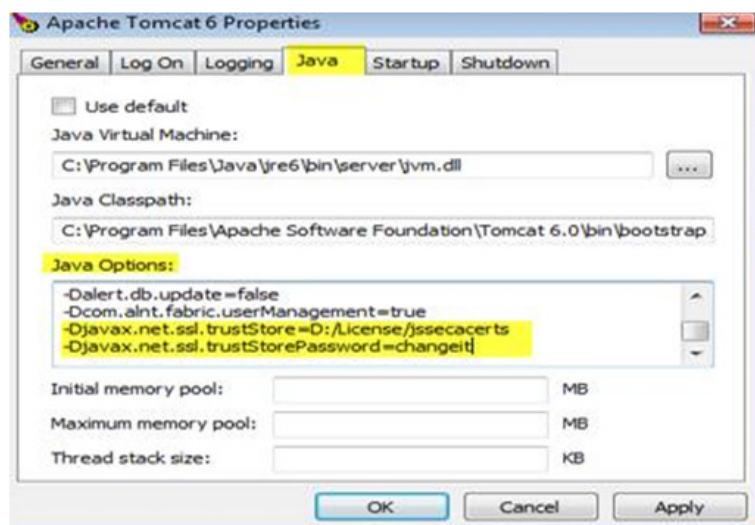
To better secure LDAP communications between AlertEnterprise Enterprise Guardian and the directory servers, we have configured such communications to use SSL encryption. Specifically, the LDAPS protocol has been configured. The steps to configure LDAPS for each connection to a directory server are as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

1. Create a `D:\cert\` folder on your system.
2. Place certificate jar file inside that folder.
3. Open the command prompt in administrator mode and perform the command:
4. Download certificate from directory server using the following command:

```
java -cp ALNTADCertUtil.jar com.alnt.ADCertInstaller
<IP_Address_Of_Directory_Server>:636
```

This creates the `jssecacerts` file in `D:\cert\` folder.

5. Add the following D parameters in `<Tomcat Installation Folder>/bin/Tomcat6w`
- ```
-Djavax.net.ssl.trustStore=D:/License/jssecacerts
-Djavax.net.ssl.trustStorePassword=changeit
```



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

## 2.2 HyTrust Cloud Control

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

### 2.2.1 How Its Used

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

### 2.2.2 Virtual Machine Configuration

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

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

VCenter Server:

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

HTCC:

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

#### Network Configuration (VCenter Server)

IPv4 Manual  
IPv6 Disabled  
IP Address: 192.168.20.6  
Netmask: 255.255.255.0  
Gateway: 192.168.20.1  
DNS Name Servers: 192.168.19.10  
DNS-Search Domains: acmefinancial.com

#### Network Configuration (HTCC)

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

### 2.2.3 Installing Vcenter Server

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

## 2.2.4 Configuring Vcenter Server

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

ESXi Host:

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

## 2.2.5 Deploying HTCC

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

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

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

## 2.2.6 Configuring HTCC

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

**Configure the HTCC Management network interface:**

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

6. Log out after network settings have been saved. This build is configured with the following settings:

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

CloudControl Setup - HyTrust CloudControl - 4.6.2.46611

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

The appliance is configured with the following settings:

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

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

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

The login screen appears.

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

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

#### HTCC Installation Wizard:

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

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



**Network Configuration**

▼ Appliance Identity and Management Interface

\*Fully Qualified Hostname (server.example.com)

\*Connection 1: IP Address

\*Connection 1: Mask

\*Gateway

\*List of DNS Server IP Addresses

▼ NTP Servers

Enable NTP Servers ☒

\*NTP Servers

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

**HyTrust CloudControl Installation Wizard**  
*Congratulations! You have completed the wizard.*

The next step is to add vCenters and hosts to the HyTrust CloudControl from the Compliance > Hosts menu. Please refer to the Installation Guide for instructions on adding your first HTCC-protected host. The Administration Guide provides instructions on converting HTCC authentication and authorization to Active Directory mode.

< Previous   Next >   Finish

### Add VCenter and Hosts to the HTCC:

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

Compliance > Hosts

Hosts

Type: All

Buttons: Add, Edit, Remove, Compliance, Update Firewall, Export as CSV, Issue Password, Cancel Password, Update Trust, Test NSX Compatibility, Download SAML Metadata

Showing 1 to 3 of 3

| Hosts                                  | Host Type                 | Patch Level                     | Label | Last Run Template | Last Run | Compliance |
|----------------------------------------|---------------------------|---------------------------------|-------|-------------------|----------|------------|
| <input type="checkbox"/> 192.168.20.12 | ESXi Host                 | VMware ESXi 6.0.0 build-3029758 | N/A   | N/A               | Never    | 0%         |
| <input type="checkbox"/> 192.168.20.6  | vCenter                   | 6.0.0 build-3634793             | N/A   | N/A               | N/A      |            |
| <input type="checkbox"/> 192.168.20.6  | vSphere Web Client Server |                                 | N/A   | N/A               | N/A      |            |

Copyright © 2009-2016 HyTrust Inc. All rights reserved. Pat. 8065714, 8166552, 8336079, 8539589, 8832784, 8966578.

ESXi:

\*Friendly Name

Description

\*Hostname/IP

Host Type

Protected ☒

Managed ☒

Labels

- NONE
- CoreAppliance
- DEV
- FirewallVM
- HIPAA
- INFRASTRUCTURE
- MONITORING
- PCI

Root Password Vaulting ☐

DRAFT

\*SSH Port 22

Use VI SDK Secure Port ☒

\*VI SDK Secure Port 443

Logging Aggregation ☒ Local  
☐ Explicit Syslog Server

Syslog Server

765

766 Note: Ensure that each host is protected.

Published Hostname/IP

Published IP Mask

767

768 vCenter:

\*Friendly Name 192.168.20.6

Description

\*Hostname/IP 192.168.20.6

User ID htaserviceaccount@acmefinancial.com

Password

Host Type vCenter

Protected ☒

769

\*HTTPS Secure Port 443

Use HTTPS Secure Port ☒

\*HTTP Port 80

Use VI SDK Secure Port ☒

\*VI SDK Port 80

\*VI SDK Secure Port 443

Logging Aggregation ☒ Local  
☐ Explicit Syslog Server

Syslog Server

Authentication Mode ☒ Use HTCC Service Account (default)

770

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

\*Published Hostname/IP 192.168.20.7

\*Published IP Mask 255.255.255.0

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

vSphere Web Client Server:

\*Friendly Name 192.168.20.6

Description

\*Hostname/IP 192.168.20.6

User ID htaserviceaccount@acmefinancial.com

Password ••••

Host Type Web Client Server

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 192.168.20.7

\*Published IP Mask 255.255.255.0

## 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.

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

786 To convert HTCC to Directory Service mode:

- 787      1. Open the Authentication Configuration page (**Configuration > Authentication**).
- 788      2. Select the **Directory Service** radio button and click **Apply**.

*Configuration > Authentication Configuration*

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

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

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

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

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

4. Click **Next**.

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

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

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

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

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

## 2.2.8 Creating and Deploying Access Policies

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

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

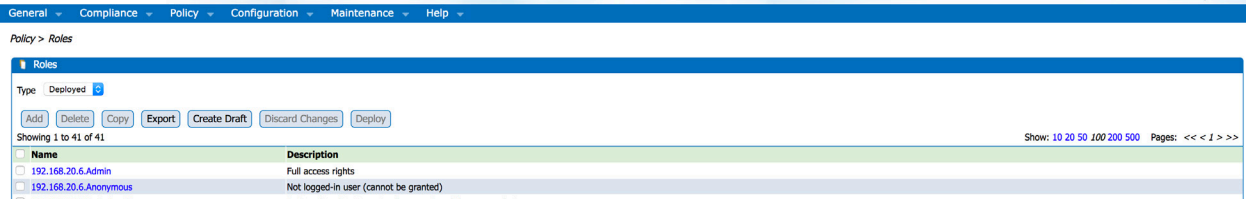
Any time a new virtual machine is created or a new host is added, the new object is automatically added to the HTCC policy and the deployed policy is enforced on the new object. To view the current policy, navigate to **Policy>Resources**. The *Deployed* policy is the policy that is currently in effect.

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

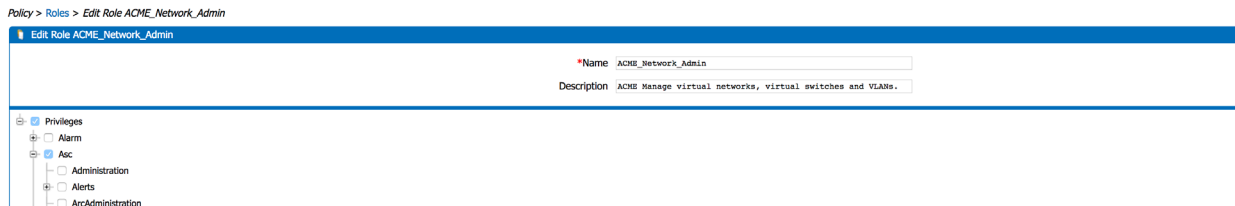
1. Open any **Policy** page.
2. Click the **Create Draft** button. This copies the "Deployed" policy to a "Draft" policy.
3. Make your desired changes to the Draft policy using the various policy pages.
4. Click the **Deploy** button to replace the current Deployed policy with the Draft policy.

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

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



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



4. Select all of the following permissions:

- a. **Asc>NxOsConfig, NxOsShow, NxOsXmlApi,ssh,storage**
- b. **DVPortgroup>Entire List** (Note: This configuration item is deprecated in versions 5.1 and above of the product.)
- c. **DVSwitch>Entire List**
- d. **DataCenter>IpPoolConfig,IpPoolQueryAllocations,IpPoolReleaseIp**
- e. **Global>CancelTask,LogEvent**
- f. **Host>Config>AdvancedConfig,NetService,Network,PciPassthru**
- g. **Network>Assign,Delete,Router**
- h. **Resource>Delete**
- i. **System>Entire List**
- j. **Task>Entire List**
- k. **VirtualMachine>Config>ManagedBy,MultiActions**

5. Press **OK**.

6. Press **Deploy**.

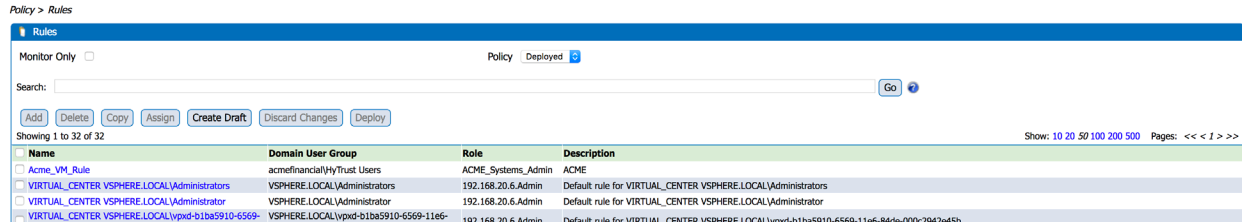
7. Repeat Steps 2–6 to create the system admin role, but with the following permissions selected:

- a. **Global>CancelTask,LogEvent**
- b. **System>Entire List**
- c. **Task>Entire List**
- d. **VApp>Entire List**
- e. **VirtualMachine>Entire List**

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

8. Navigate to **Policy>Rules**.

9. Select **Create Draft**.



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

**Constraints**

Showing 0 to 0 of 0

| Edit             | Constraint Type | Description |
|------------------|-----------------|-------------|
| No Records Found |                 |             |

**Assigned Resources**

Showing 1 to 2 of 2

| Name           | Description                                    |
|----------------|------------------------------------------------|
| 192.168.20.6   | Folder:group-d1 @ https://192.168.20.6/443/sdk |
| Appliance Root |                                                |

**Assigned RuleSets**

Showing 0 to 0 of 0

| Name             | Description |
|------------------|-------------|
| No Records Found |             |

OK Cancel

11. Select **Assign**.

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

**Results**

| Current Rules                                                                                                                                               | Current RuleSets                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> Web Client<br><input type="checkbox"/> Server 192.168.20.6<br><input checked="" type="radio"/> HyTrust CloudControl Appliance Root | Rule(s): Default VMUser rule<br>Rule(s): Default ARCAAdmin rule, Acme_VM_Rule2, Default SecurityAdmin rule, Default SecurityAuditor rule, Default RoleAdmin rule, Default UCS rule, Default DCAdmin rule, Default SuperAdmin rule, Default ThirdParty rule, Default KVMAdmin rule, Acme_VM_Rule, Default ESXAdmin rule, Default AppAdmin rule, Default NetworkEngineer rule, Default NetworkAdmin rule, Default CoreAppAdmin rule, Default PolicyAdmin rule, Default LoadBalancer rule, Default NetworkOperator rule, Default StorageAdmin rule, Default VMUser rule, Default BackupAdmin rule, Default ARCAssessor rule, Default SecurityOperator rule, Default VMPowerUser rule, Default VAdmin rule |

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' active directory group.

## 2.2.9 Configure Logging

1. Select **Configuration > Logging**.

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

3. Select **External**.

4. Select **CEF**.

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

Configuration > Logging Configuration

The screenshot shows the 'Logging Configuration' page. The top section is 'HTCC Logging Configuration' with the following settings:
 

- Logging Level: **DEBUG** (dropdown)
- HTCC Logging Aggregation: **External** (radio button)
- Logging Aggregation Template Type: **CEF** (radio button)
- \*HTCC Syslog Servers: **192.168.17.10:514** (text field)
- Encrypt Syslog: ☐
- Manage Logs: **Download** (button)
- Repair Log: **Repair** (button)
- Log Viewer: **Reset** (button)

 The bottom section is 'Host Default Logging Configuration' with the following settings:
 

- Default Logging Aggregation: **Explicit Syslog Server** (radio button)
- \*Default Syslog Server: **192.168.17.10:514** (text field)

 An 'Apply' button is located at the bottom right of the form.

878 6. Select **Explicit Syslog Server**.

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

881 8. Select **Apply**.

## 882 2.3 Microsoft Active Directory

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

### 884 2.3.1 How It's Used

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

### 890 2.3.2 Virtual Machine Configuration

891 The AD virtual machine is configured as follows:

- 892 ☐ 1 CPU Core
- 893 ☐ 4GB RAM
- 894 ☐ 84GB HDD
- 895 ☐ 2 Network Adapters

#### 896 Network Configuration (Interface 1)

897 IPv4 Manual  
 898 IPv6 Disabled  
 899 IP Address: 192.168.19.10  
 900 Netmask: 255.255.255.0  
 901 Gateway: 192.168.19.1  
 902 DNS Name Servers: 192.168.19.10  
 903 DNS-Search Domains: AcmeFinancial.com

### 904 2.3.3 Installing AD



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

906 [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-)  
 907 [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-)

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

### 909 2.3.4 DNS Configuration

910 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   |

911 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 |

### 912 2.3.5 Installing Splunk Universal Forwarder

913 *Note:* You will need a Splunk account to download the Splunk Universal Forwarder. It is free and can be  
 914 set up at: [https://www.splunk.com/page/sign\\_up](https://www.splunk.com/page/sign_up)

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

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

### 2.3.6 Install Security Compliance Manager

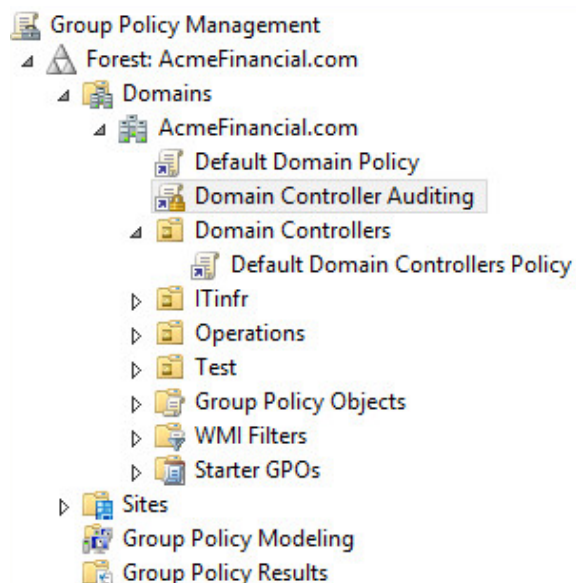
Install Microsoft Security Compliance Manager: <https://www.microsoft.com/en-us/download/details.aspx?id=53353>

### 2.3.7 Group Policy Object (GPO) Configuration

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

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

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

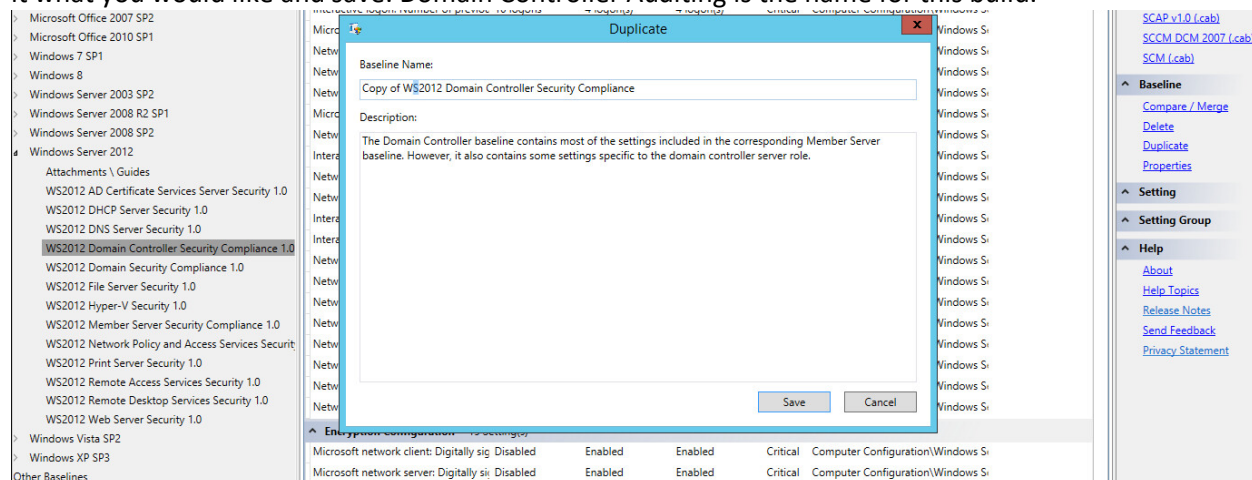


For this build, no changes are made to the Default Domain or Default Domain Controllers Policy. Both policies are “enabled” and “link enabled.”

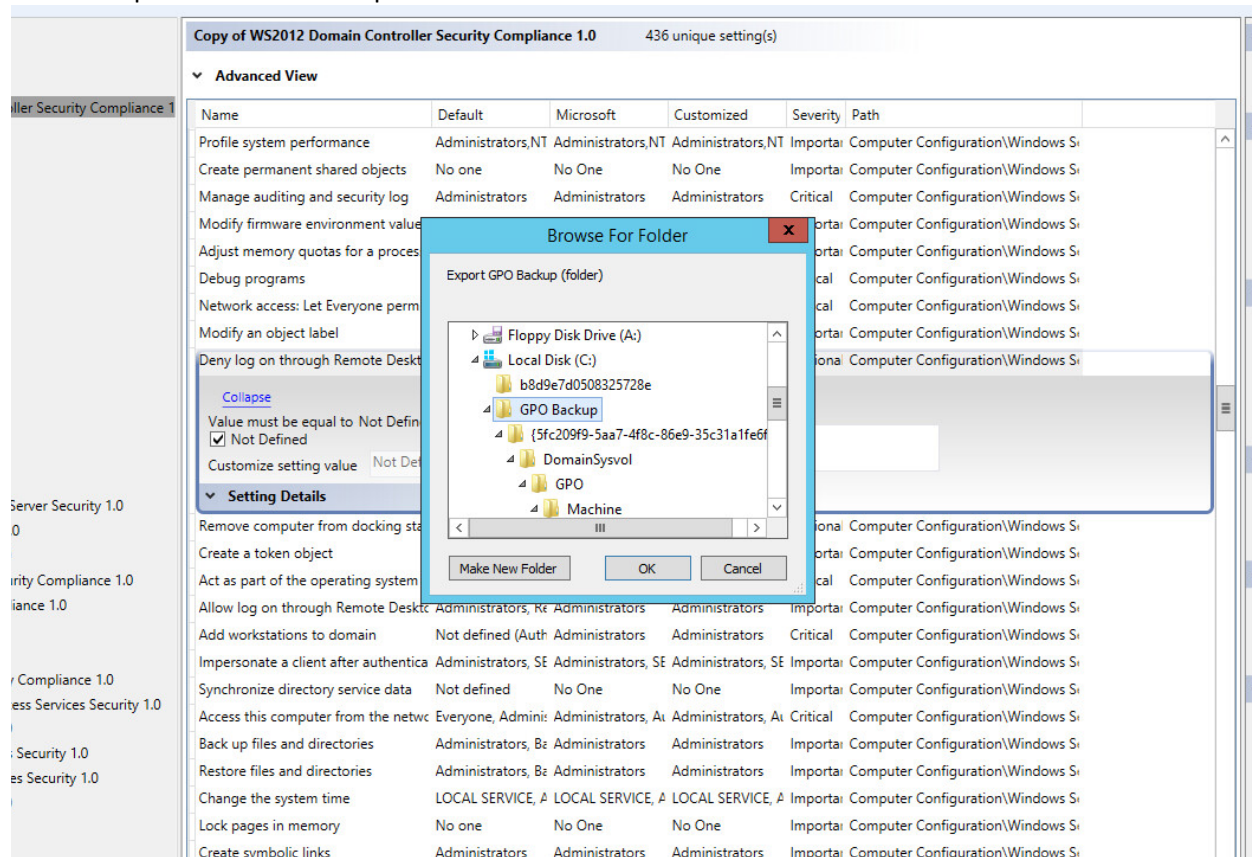
Minor changes are made to the Domain Controller Auditing Policy to enable the ability to audit user account changes, attribute changes, and policy changes for this build.

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

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

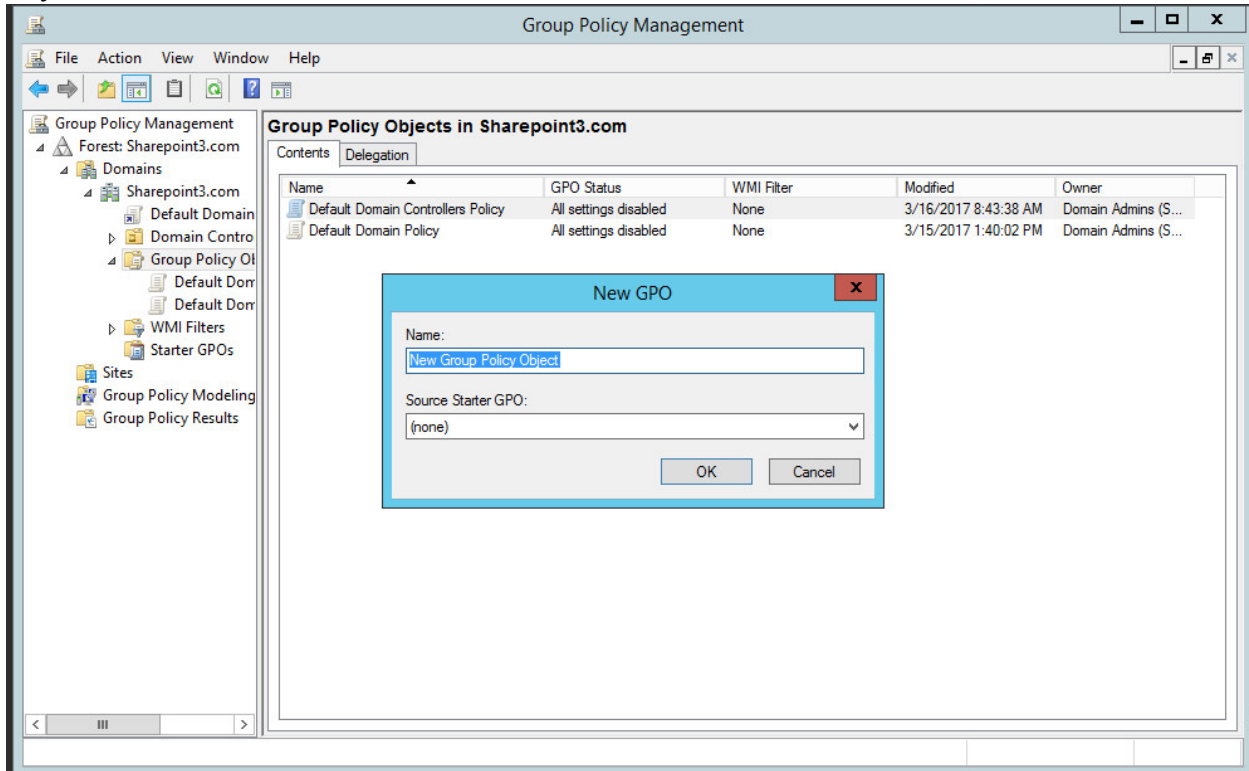


- 942 2. Export to a GPO backup folder.  
943

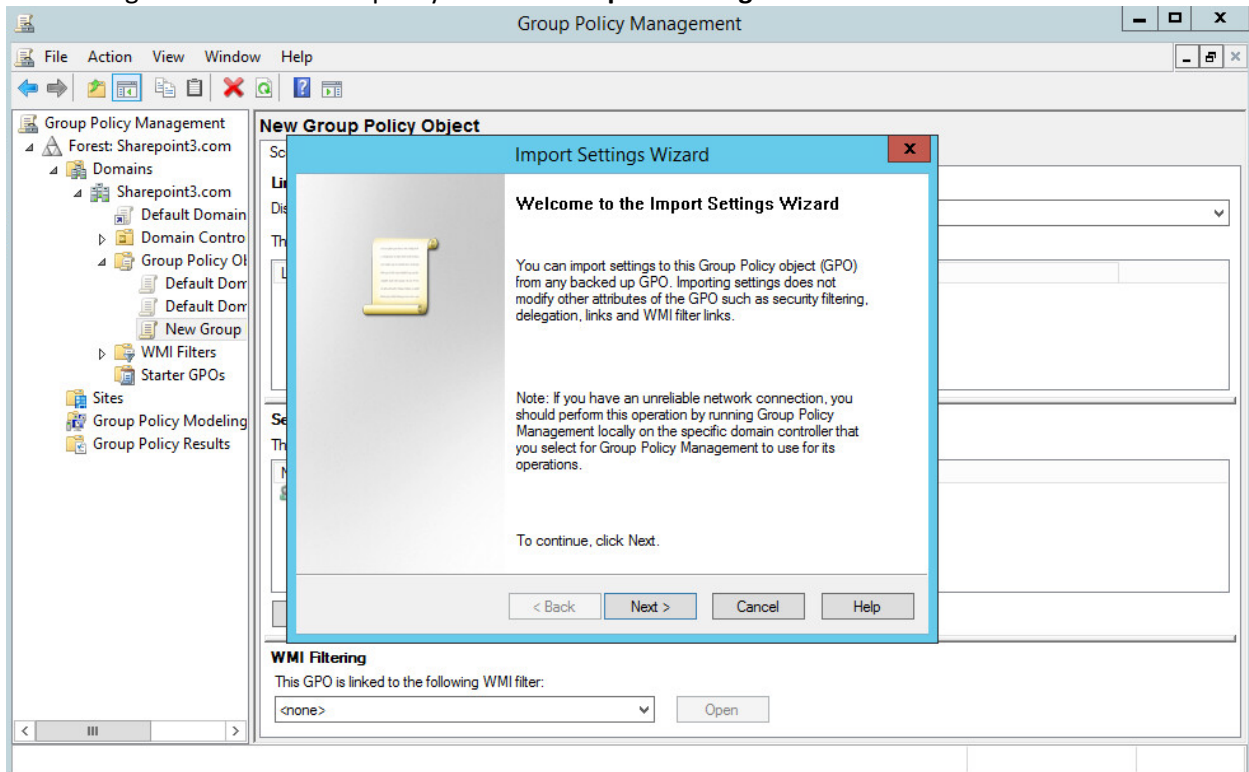


DRAFT

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

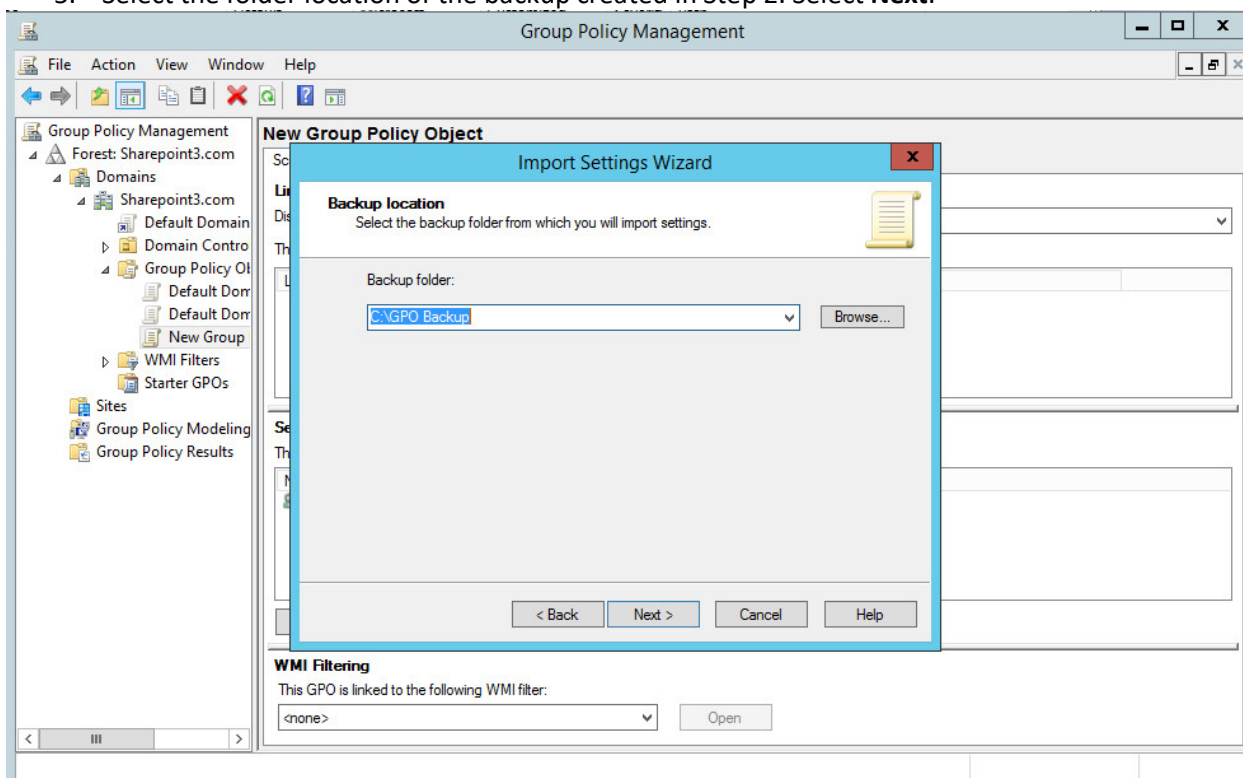


- 947 4. Right-click on the new policy and select **Import Settings**. Click **Next**.  
948

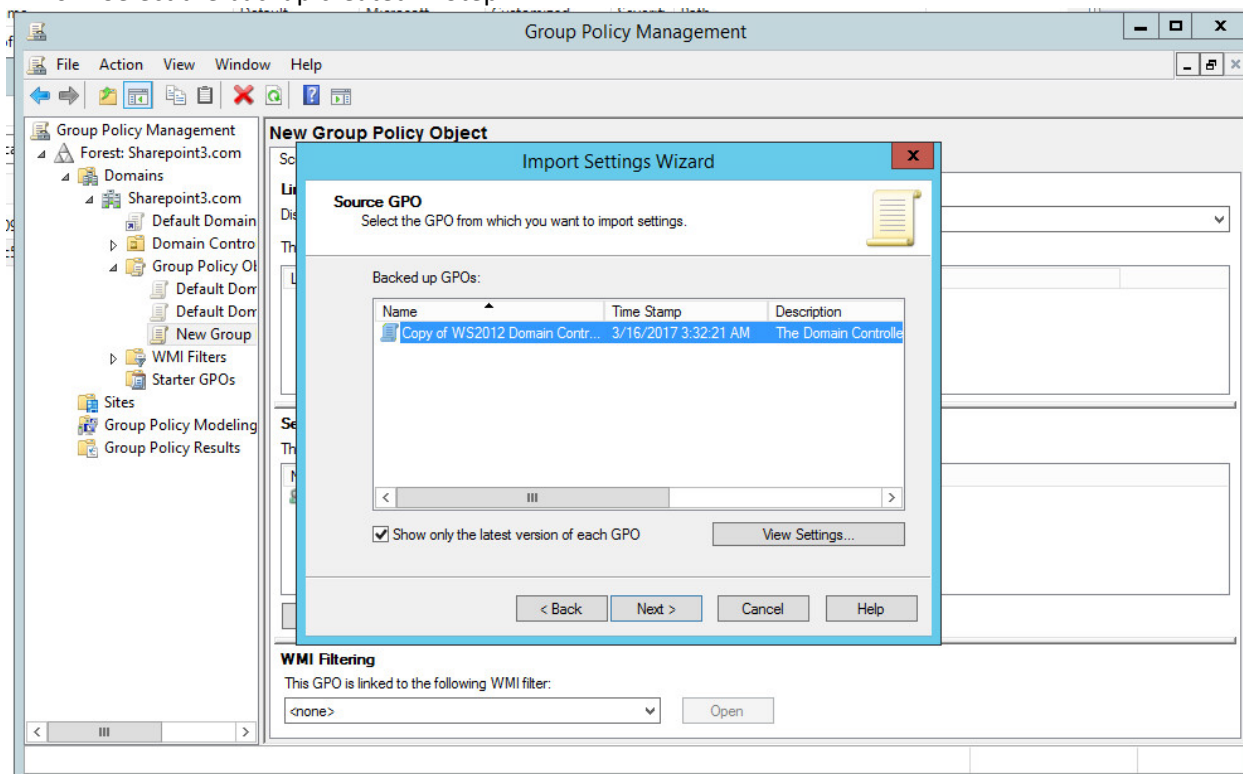


949

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

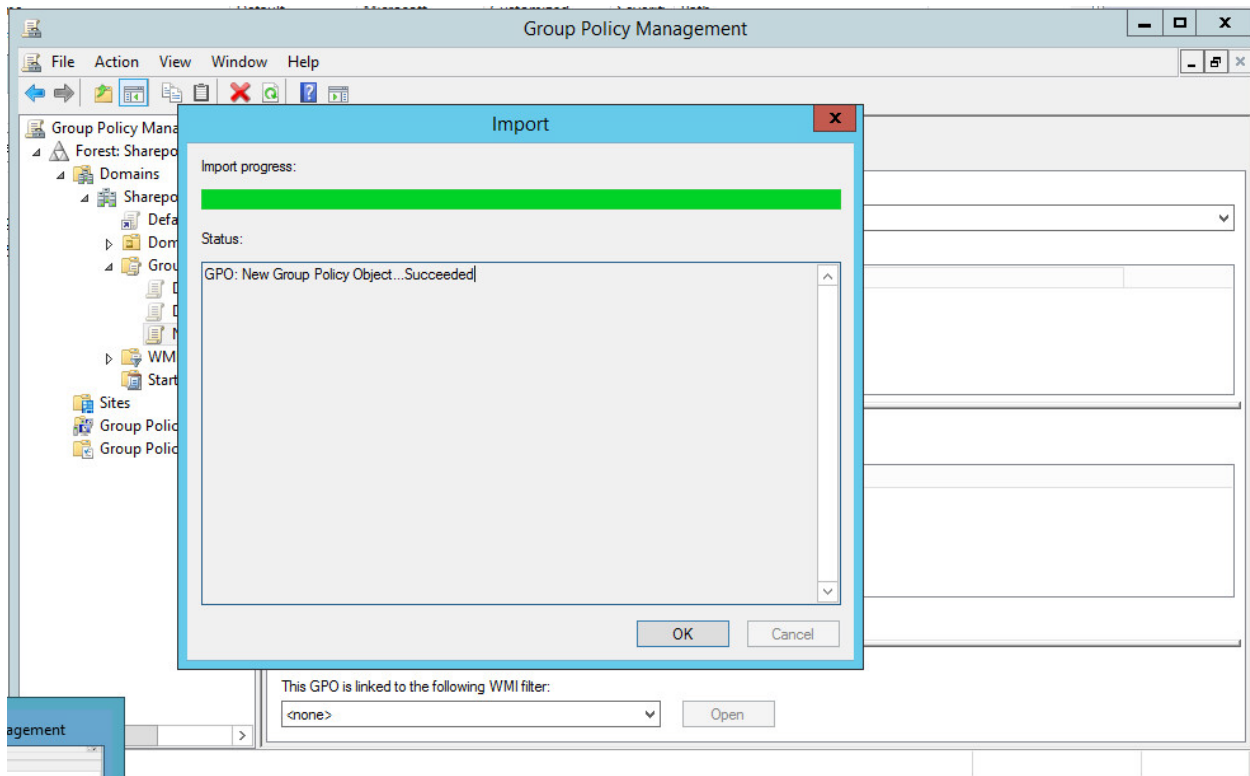
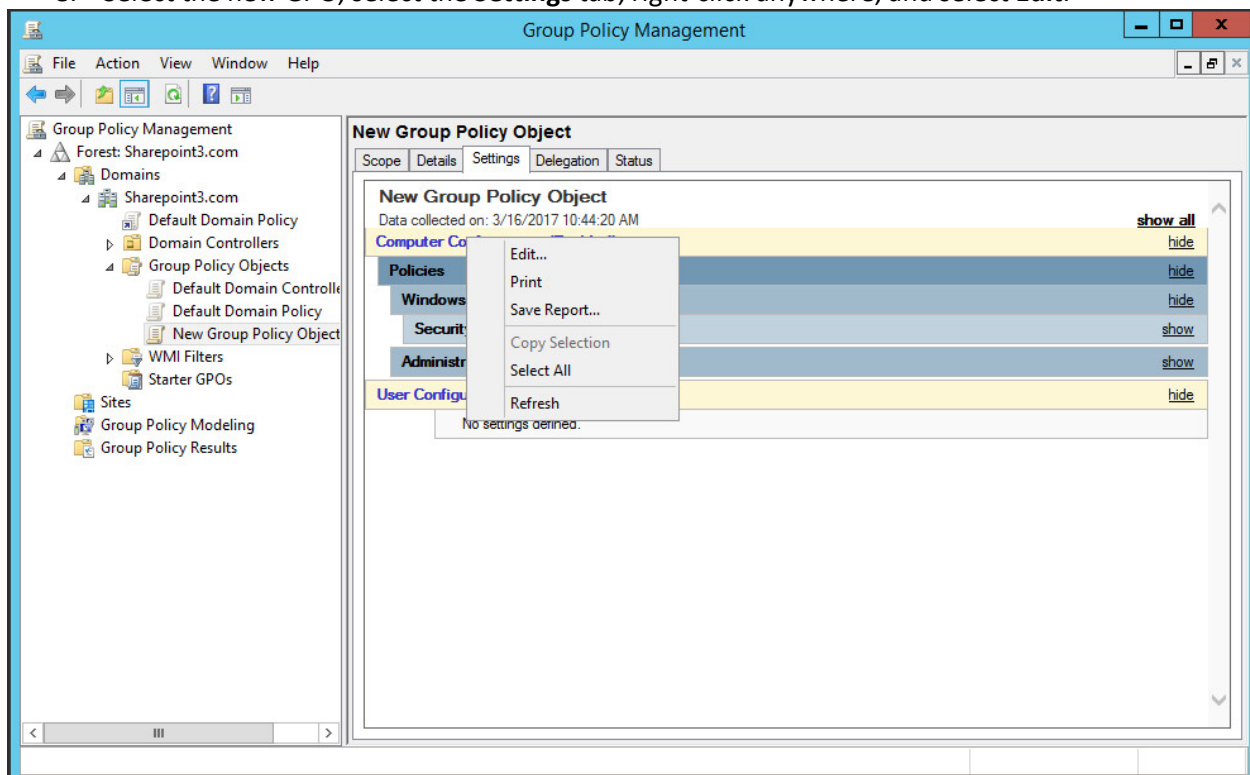


- 951 6. Select the backup created in Step 2.

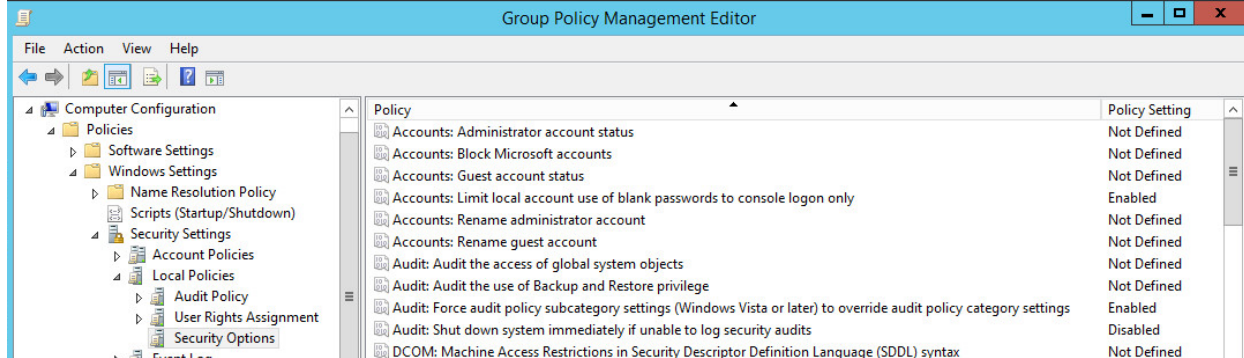


953



7. Click **Next** at the end of the wizard and **Finish**.8. Select the new GPO, select the **Settings** tab, right-click anywhere, and select **Edit**.9. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies>Security Options**. Change the value for "Audit: Force audit policy subcategory settings

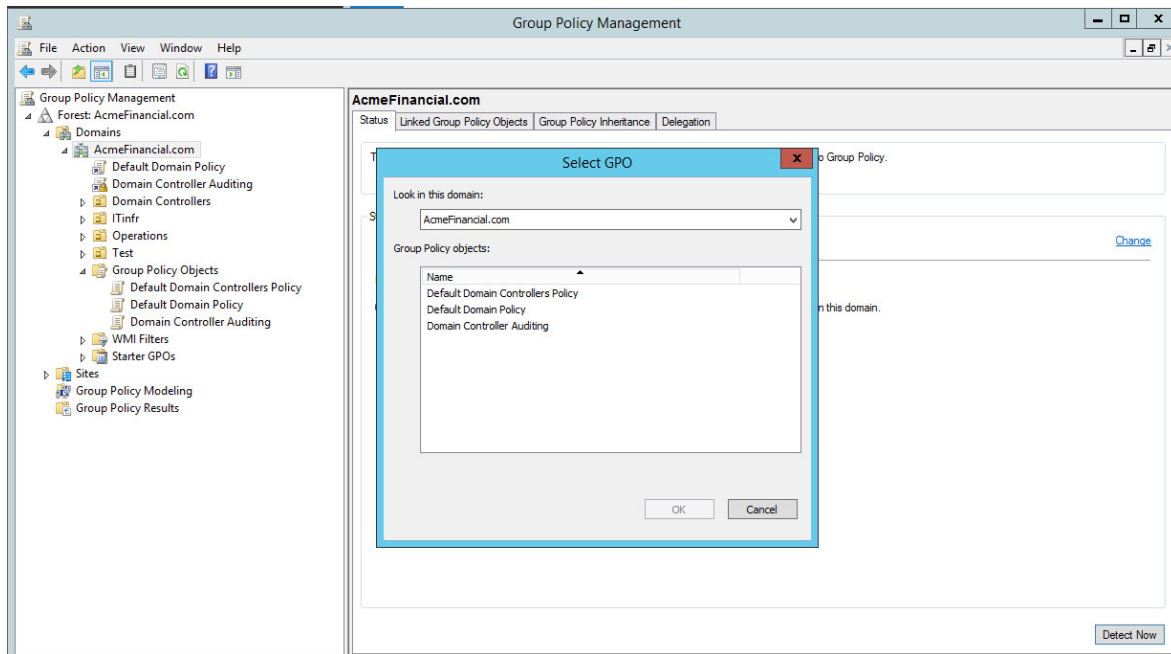
960 (Windows Vista or later) to override audit policy category settings” to “Enabled.” Change the value for  
 961 “Domain controller: LDAP server signing requirements” to “require signing.”



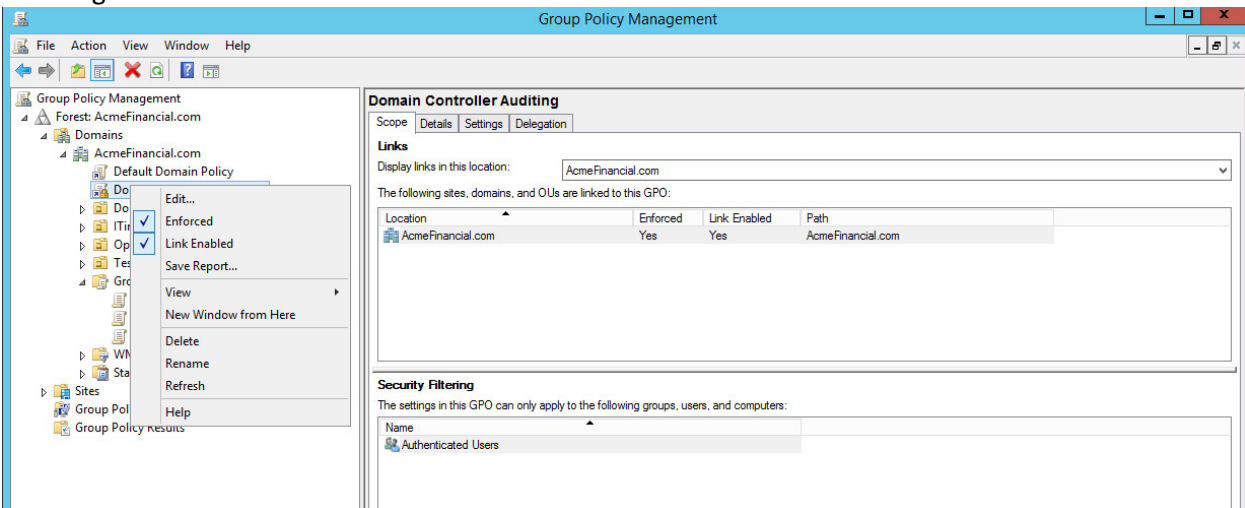
- 962 10. Navigate to **Computer Configuration>Policies>Windows Settings>Security Settings>Advanced**  
 963 **Audit Policy Configuration>Audit Policies**. Make the following changes and save:  
 964

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

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

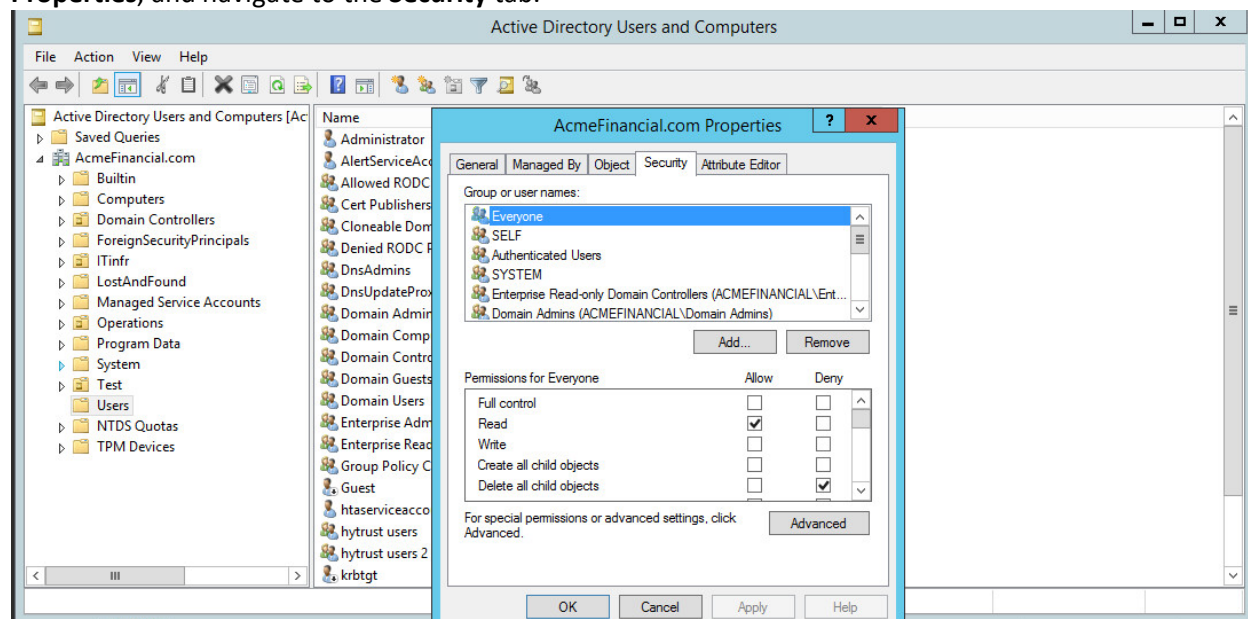


- 967 12. Right-click on the new GPO linked directly under the top-level domain and select **Enforced** by  
 968 checking it on the left.

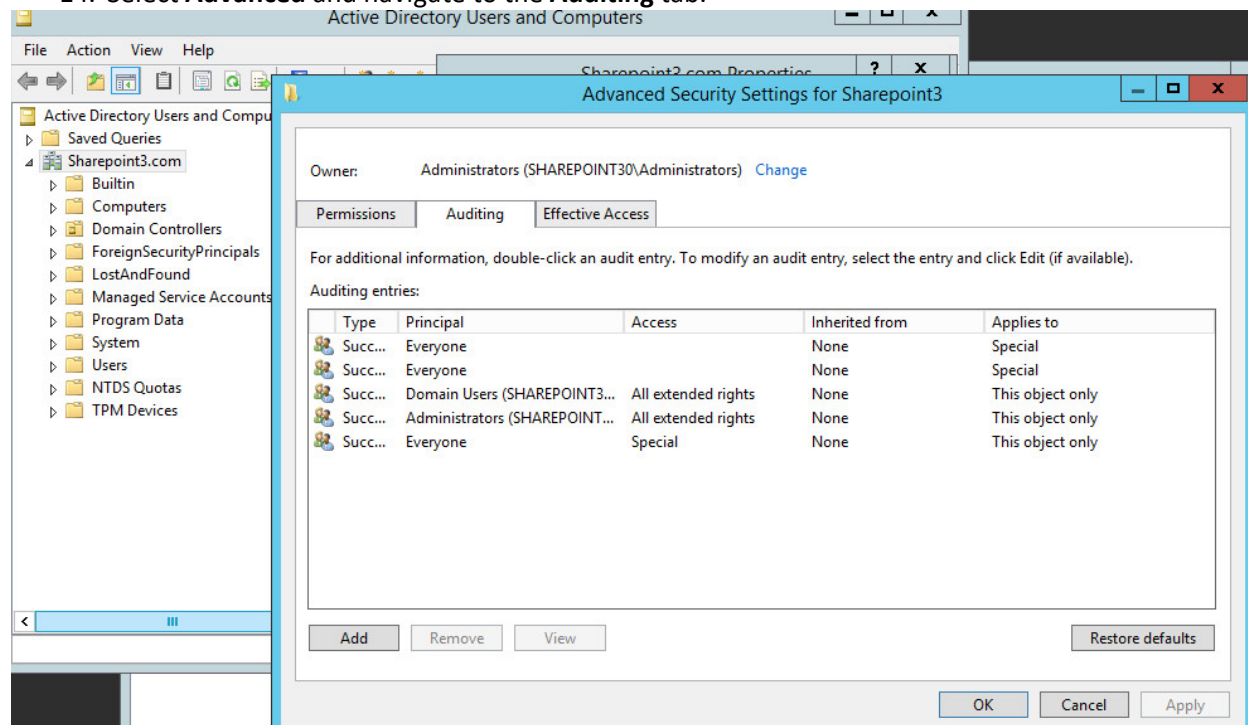




13. Open **Active Directory Users and Computers**, right-click on the top level of the domain, select **Properties**, and navigate to the **Security** tab.

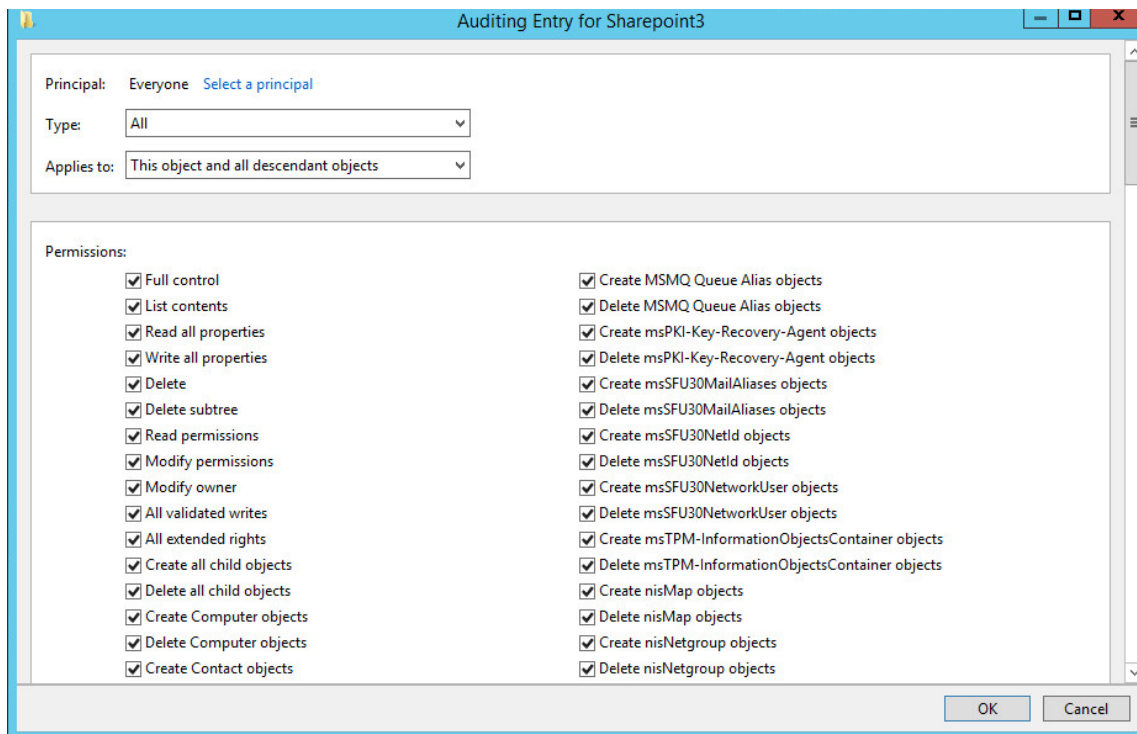


14. Select **Advanced** and navigate to the **Auditing** tab.



15. Add a new entry with the following parameters:

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



### 979 2.3.8 Script: AdDOnlineStatus.ps1

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

```

982 #This script determines if this server is online or offline
983 #If a gateway route exists, the script will
984 #output the current time, hostname, status and previous time (last
985 #time it wrote to output file)
986 #Check if gateway route exists
987 if (Get-Netroute 0.0.0.0/0)
988 {
989     #Store date in PrevTime variable
990     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
991     #Check if prevtime-file.txt exists
992     if (ls C:\scripts\prevtime-file.txt)
993     {
994         #Place the contents of prevtime-file.txt in the PrevTime variable
995         $PrevTime=Get-Content C:\scripts\prevtime-file.txt
996     }
997     #Place the current date in CurrentTime
  
```

```

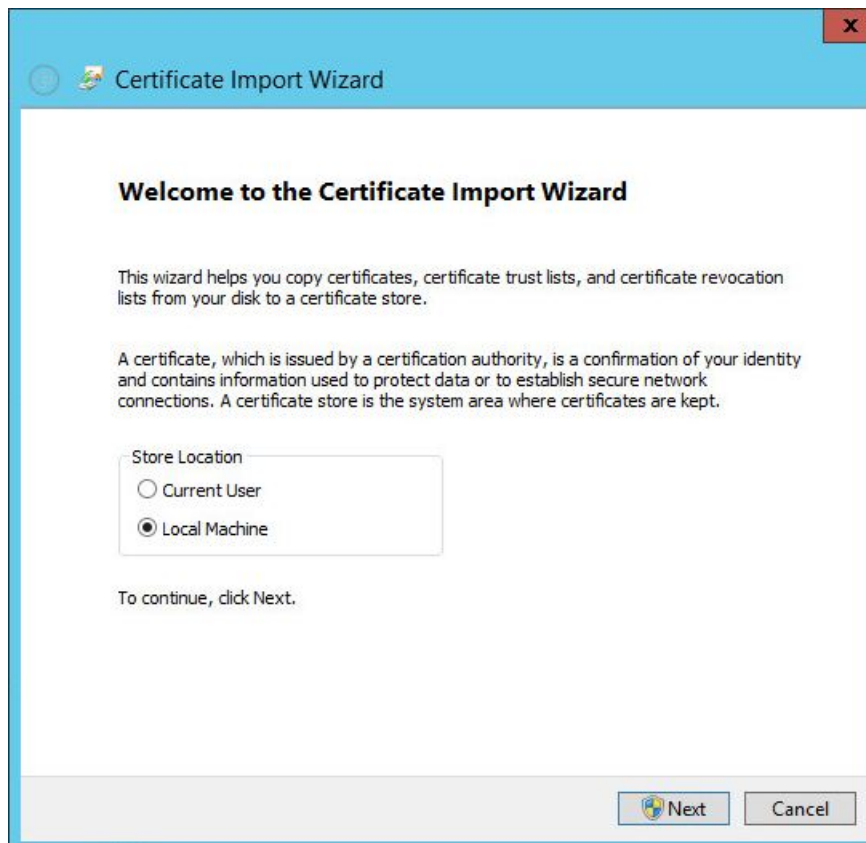
998     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
999     #Overwrite the contents of prevtime-file.txt with the current date
1000     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\prevtime-file.txt
1001     $HostVar = hostname
1002     $Status = 'online'
1003     #Add the contents of the variables CurrentTime, HostVar, Status, PrevTime to
1004     Radiant-Status-Output.csv
1005     Add-Content C:\scripts\AD-Status-Output.csv
1006     $CurrentTime','$HostVar','$Status','$PrevTime
1007     }
1008 else
1009     {
1010     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1011     if (ls C:\scripts\prevtime-file.txt)
1012     {
1013         $PrevTime=Get-Content C:\scripts\prevtime-file.txt
1014     }
1015     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
1016     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\prevtime-file.txt
1017     $HostVar = hostname
1018     $Status = 'offline'
1019     Add-Content C:\scripts\AD-Status-Output.csv
1020     $CurrentTime','$HostVar','$Status','$PrevTime
1021     }

```

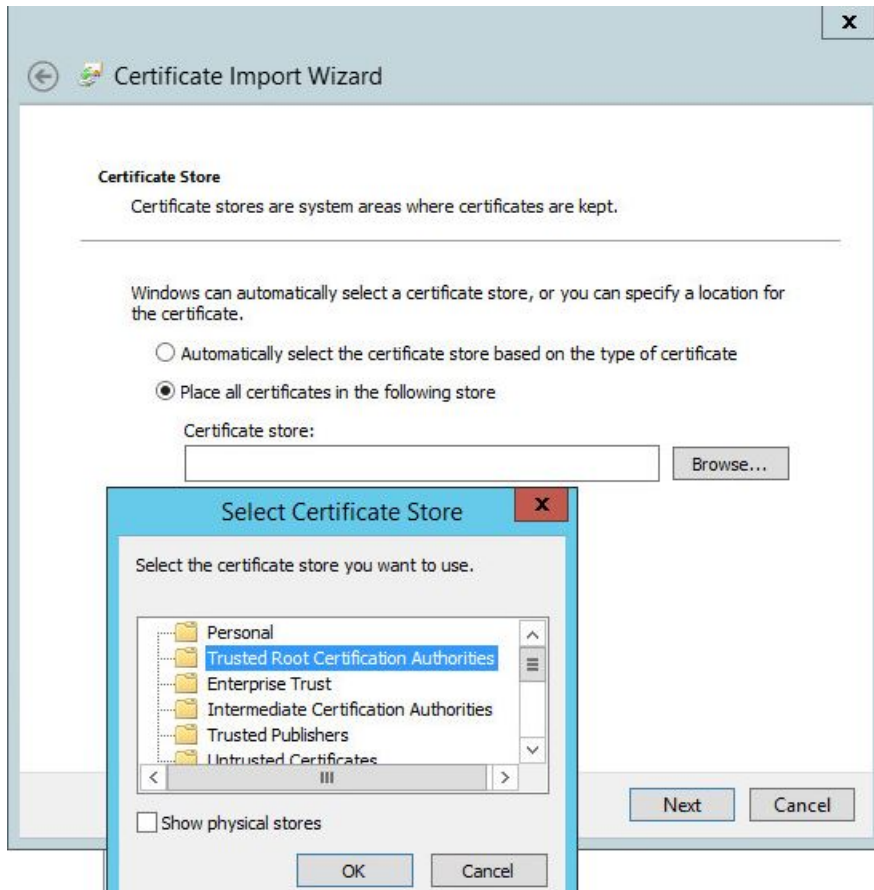
### 1022 2.3.9 LDAPS Configuration

1023 Once installed, the Active Directory service listens for both LDAP and LDAPS connections. To make  
 1024 LDAPS active, you will need to make sure that the certificates for the Active Directory domain controller  
 1025 and the certificate authority (CA) that signed the certificate are properly installed. Once these  
 1026 certificates are imported, LDAP clients will be able to use the LDAPS service.

- 1027 1. Copy the CA and domain controller certificates over to the Active Directory domain controller.
- 1028 2. Right-click on each certificate and choose **Install Certificate**.
- 1029 3. Choose **Local Machine**.



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



## 2.4 NextLabs Entitlement Manager

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

### 2.4.1 How It's Used

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

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

### 2.4.2 Virtual Machine Configuration

The NextLabs virtual machine is configured with:

- Windows Server 2012 R2
- 8 CPU cores
- 16GB of RAM
- 1 NIC
- 100GB of Storage

## Network Configuration (Interface 1)

IPv4 Manual

IPv6 Disabled

IP Address: 192.168.14.117

Netmask: 255.255.255.0

Gateway: 192.168.14.1

DNS Name Servers: 192.168.14.1

DNS-Search Domains: n/a

### 2.4.3 Prerequisites

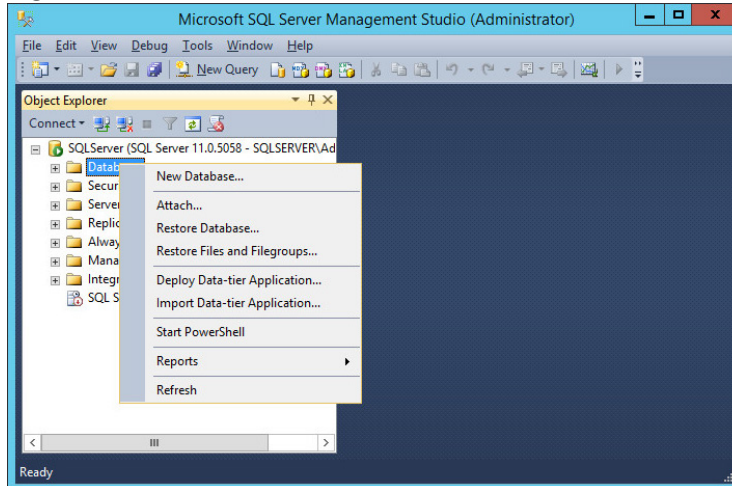
NextLabs Control Center requires an Oracle or MS SQL Server. It is recommended that the database be given 500GB of free storage space. In this build, only 100GB of storage is used for development purposes.

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

### 2.4.4 Installing NextLabs

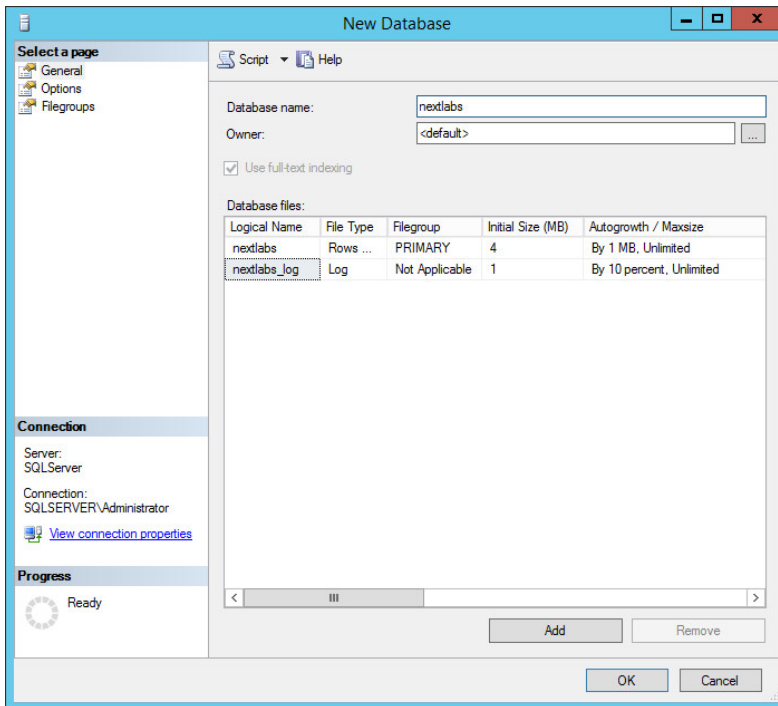
#### Control Center 7.7

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

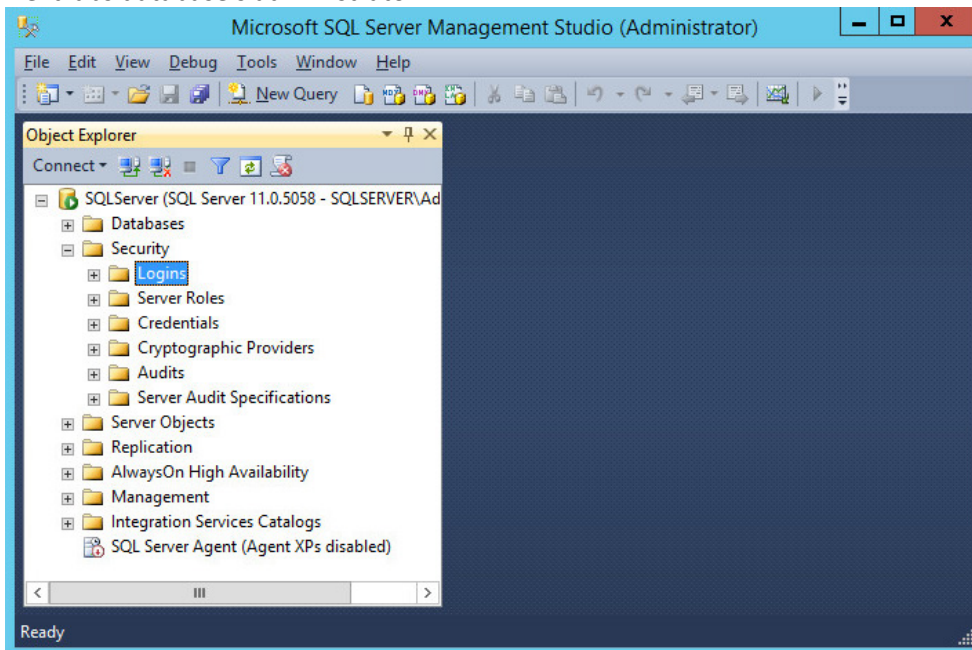


4. In the New Database window, specify a **Database name** that works for you. The application automatically copies this into the **Logical Names** of the **Database files**. Click **OK**. Example name

1079 from this build: **nextlabs**.



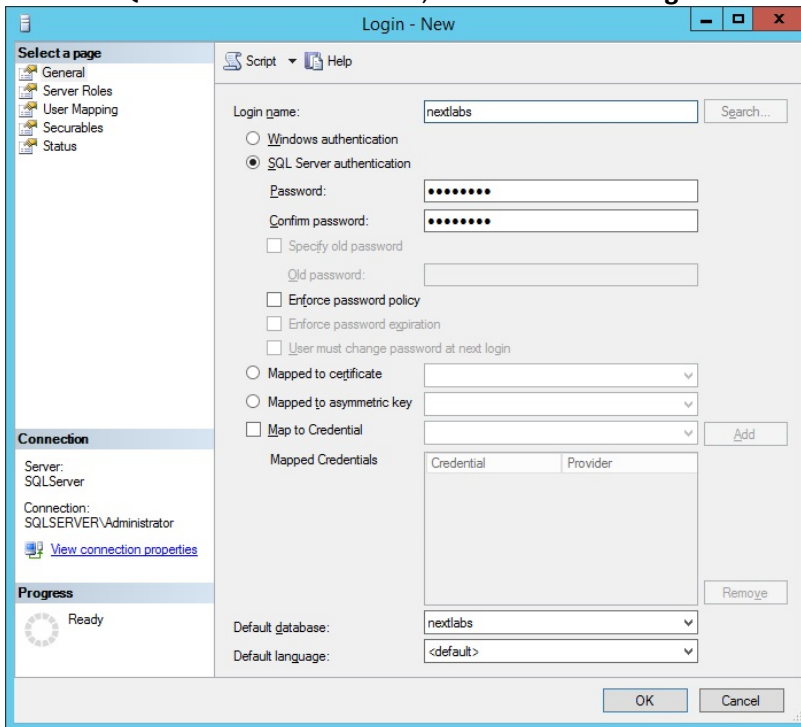
- 1080 5. Click on the menu box next to **Security** to begin the process for creating a new login for the new  
 1081 NextLabs database's administrator.  
 1082



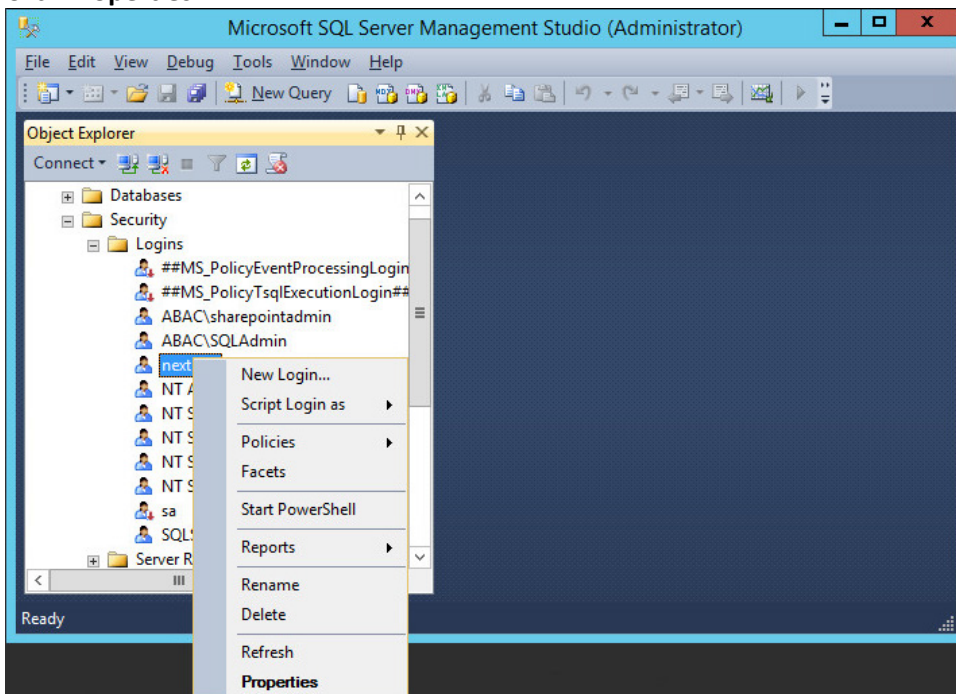
- 1083 6. Right-click **Logins**. Left-click **New Login**.  
 1084



- 1085 7. Click on **SQL Server authentication**, and enter a new **Login name** and **Password**.



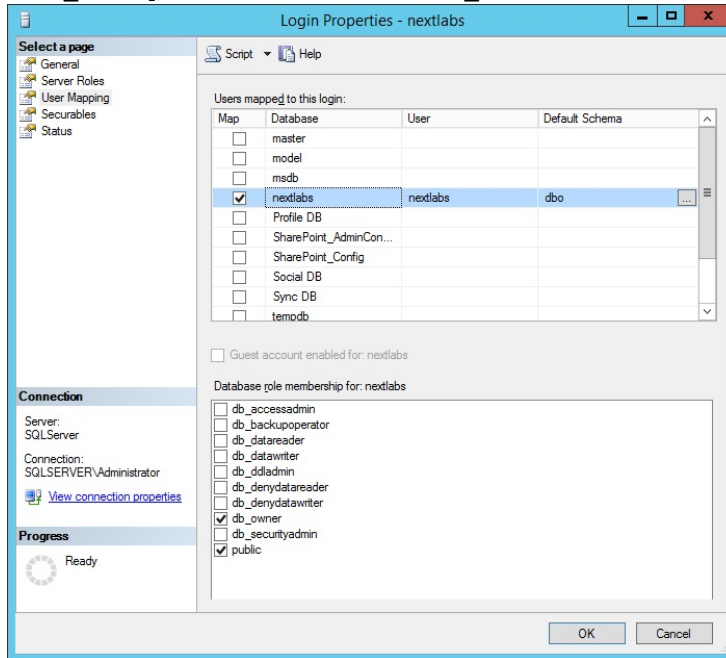
- 1086 8. Click the menu box next to **Logins**. Right-click on the new user created in the previous step.  
 1087 Click **Properties**.  
 1088



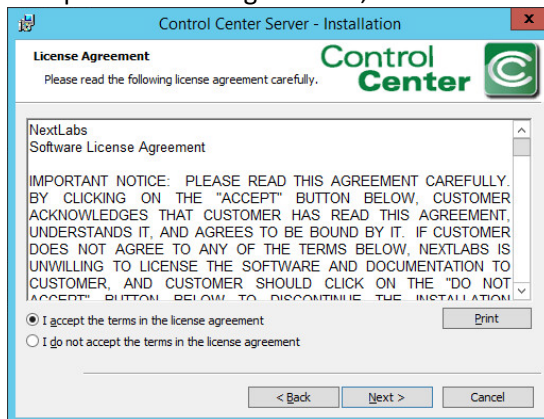
1089



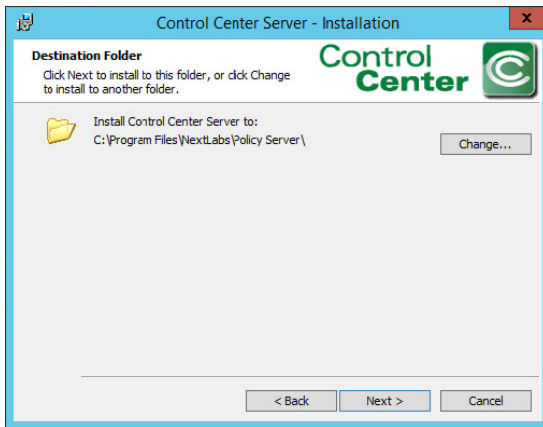
9. Click on **User Mapping**, then **New Database**. Under **Database role membership for: [database\_name]**, check the box next to **db\_owner**.



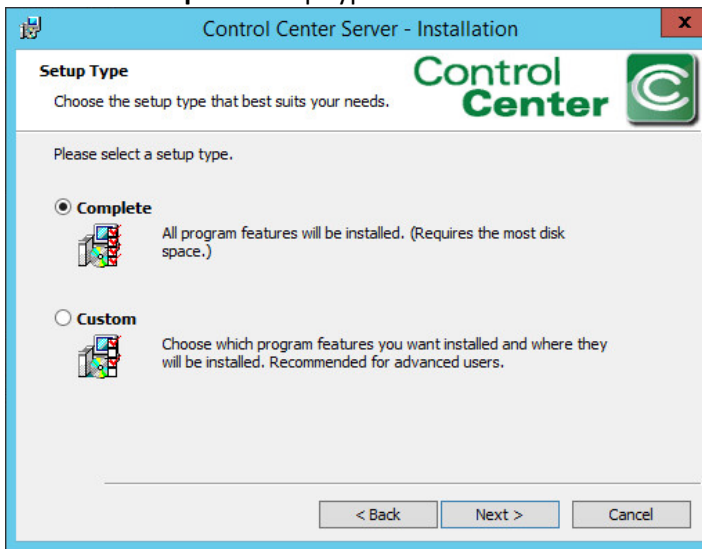
10. Locate the installation zip file, provided by NextLabs support, and extract it.
11. Run the installer as follows:
- On a Windows server, launch Command Prompt as Administrator.
  - In the command prompt, navigate to the folder that contains `install.bat`. The following is an example of the `cd` command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



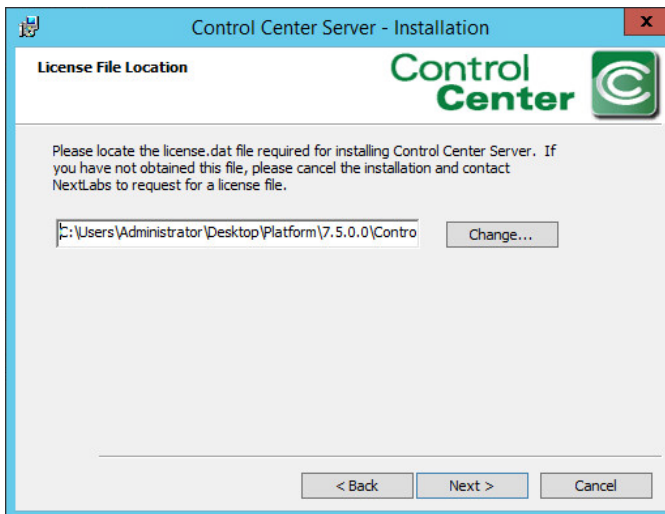
1103 15. Click **Next**.



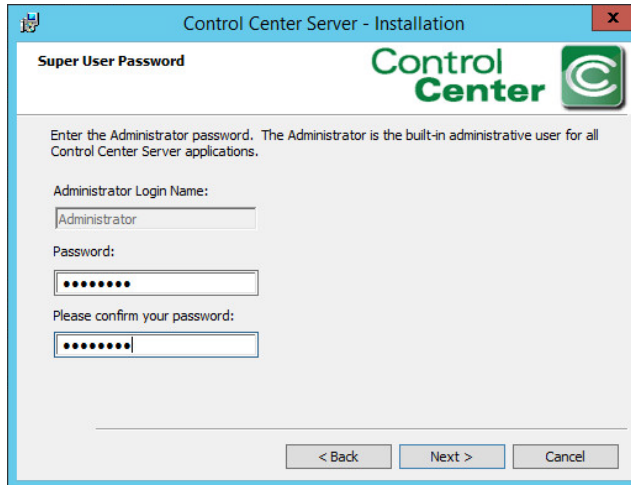
1104 16. Select the **Complete** setup type. Click **Next**.



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

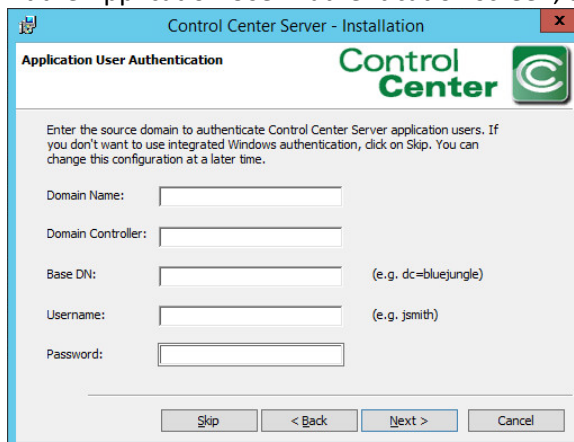


- 1109 18. Enter a Password for the built-in administrative user for all Control Center Server applications.  
 1110 Click **Next**.



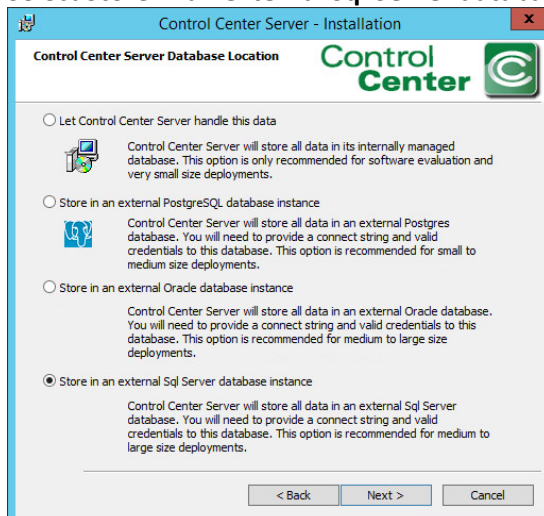
The screenshot shows the 'Control Center Server - Installation' window with the 'Super User Password' tab selected. The window title is 'Control Center Server - Installation'. The Control Center logo is in the top right. The text reads: 'Enter the Administrator password. The Administrator is the built-in administrative user for all Control Center Server applications.' Below this are three input fields: 'Administrator Login Name:' (containing 'Administrator'), 'Password:' (masked with dots), and 'Please confirm your password:' (masked with dots). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

- 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



The screenshot shows the 'Control Center Server - Installation' window with the 'Application User Authentication' tab selected. The window title is 'Control Center Server - Installation'. The Control Center logo is in the top right. The text reads: 'Enter the source domain to authenticate Control Center Server application users. If you don't want to use integrated Windows authentication, click on Skip. You can change this configuration at a later time.' Below this are five input fields: 'Domain Name:', 'Domain Controller:', 'Base DN:' (with example '(e.g. dc=bluejungle)'), 'Username:' (with example '(e.g. jsmith)'), and 'Password:'. At the bottom are four buttons: 'Skip', '< Back', 'Next >', and 'Cancel'.

- 1115 22. Select **Store in an external Sql Server database instance**. Click **Next**.  
 1116

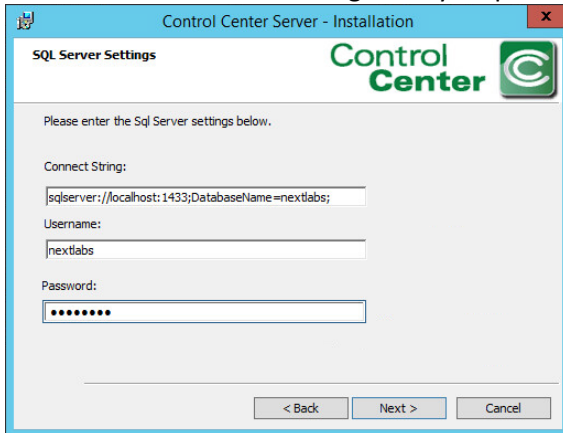


The screenshot shows the 'Control Center Server - Installation' window with the 'Control Center Server Database Location' tab selected. The window title is 'Control Center Server - Installation'. The Control Center logo is in the top right. The text reads: 'Control Center Server Database Location'. There are four radio button options:
 

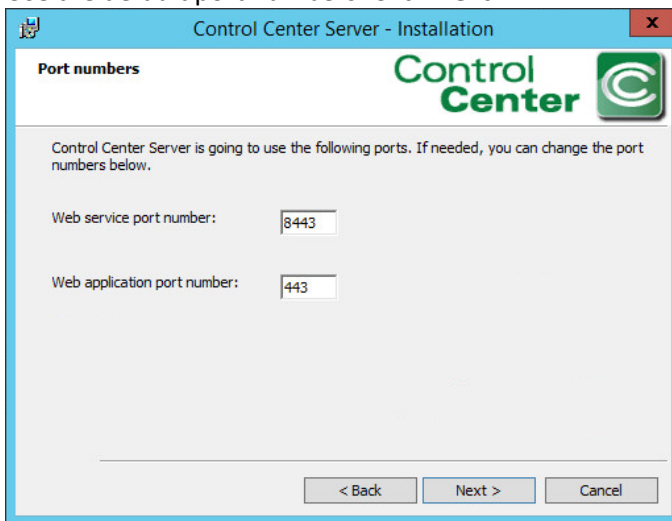
- ☐ Let Control Center Server handle this data. Control Center Server will store all data in its internally managed database. This option is only recommended for software evaluation and very small size deployments.
- ☐ Store in an external PostgreSQL database instance. Control Center Server will store all data in an external Postgres database. You will need to provide a connect string and valid credentials to this database. This option is recommended for small to medium size deployments.
- ☐ Store in an external Oracle database instance. Control Center Server will store all data in an external Oracle database. You will need to provide a connect string and valid credentials to this database. This option is recommended for medium to large size deployments.
- ☒ Store in an external Sql Server database instance. Control Center Server will store all data in an external Sql Server database. You will need to provide a connect string and valid credentials to this database. This option is recommended for medium to large size deployments.

 At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

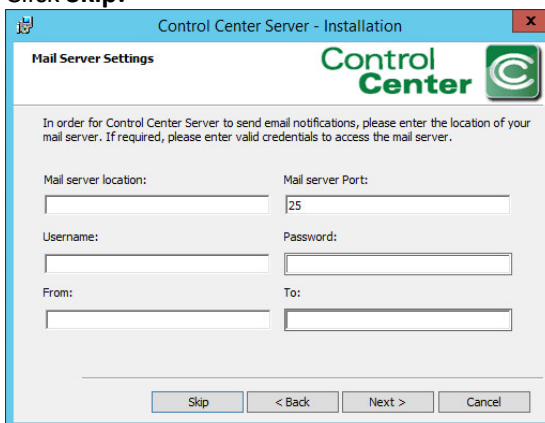
- 1118 23. At the SQL Server settings screen, specify the **Connect String**, **Username**, and **Password**. Make  
1119 sure the SQL Server is running. It may help to restart the SQL Server.



- 1120 24. Use the default port numbers. Click **Next**.  
1121

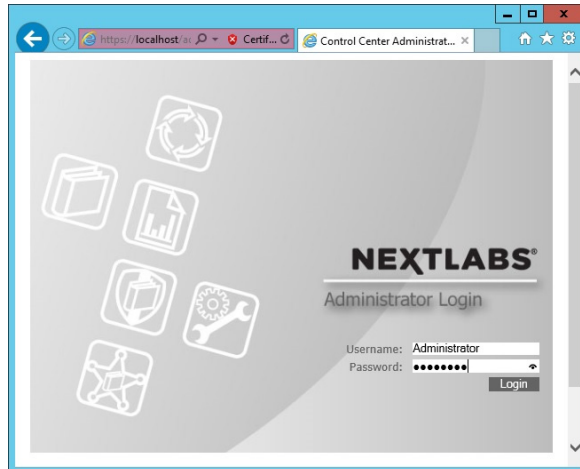


- 1122 25. Click **Skip**.  
1123



- 1124 26. Click **Install**.  
1125  
1126 27. Once completed, click **Finish**.  
1127 28. Open an Internet browser, navigate to <https://localhost/administrator>, and log in to the Control  
1128 Center Administrator web application.

- 1129 a. Enter the Administrator Username and Password to log in.

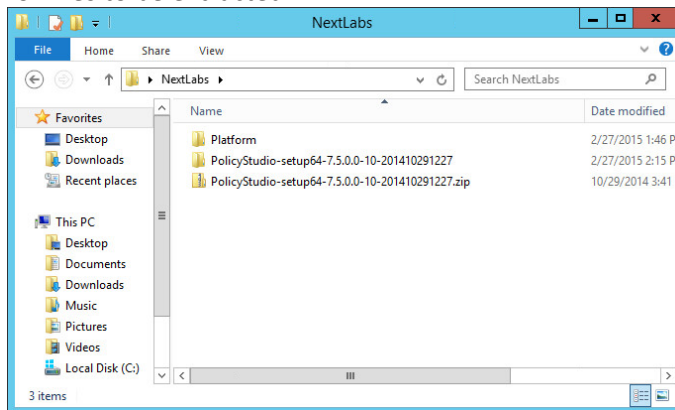


- 1130  
1131 29. Once logged in to the Control Center Administrator web application in your browser, you can  
1132 verify that the NextLabs Control Center is installed and configured correctly on the SQL Server.

### 1133 Policy Studio 7.7

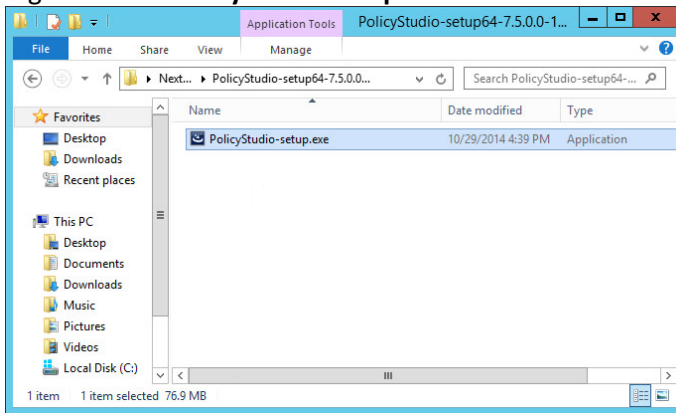
1134 Complete the standard Policy Studio installation per NextLabs documentation available to customers  
1135 using the following steps:

- 1136 1. On the same server, go to your desktop or other known location where the required NextLabs  
1137 Policy Studio installation files are stored.  
1138 2. Right-click on **PolicyStudio-setup64-7.5.0.0-10-201410291227.zip** and select **Extract All**. Wait  
1139 for files to be extracted.

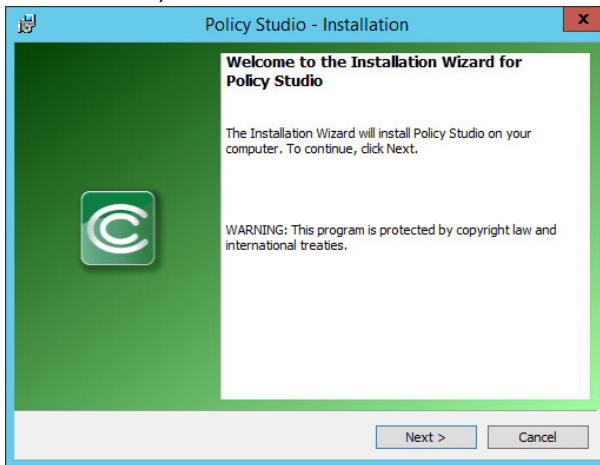


- 1140  
1141 3. Double-click to open the **PolicyStudio-setup64-7.5.0.0-10-201410291227** folder.

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



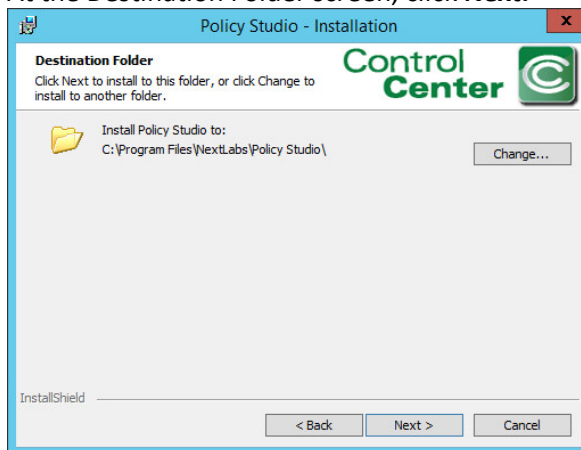
5. At the Welcome to the Installation Wizard for Policy Studio screen of the Policy Studio Installation Window, click **Next**.



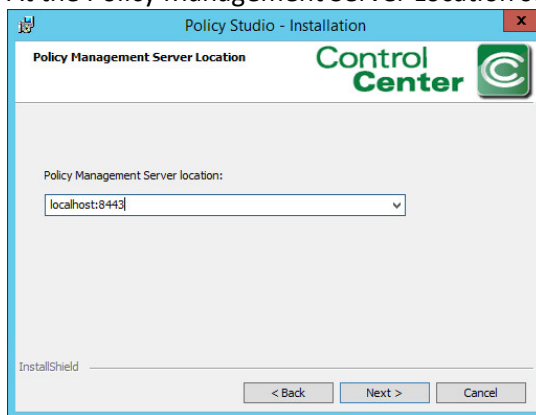
6. At the License Agreement screen, select **I accept the terms in the license agreement**, and click **Next**.



- 1150 7. At the Destination Folder screen, click **Next**.

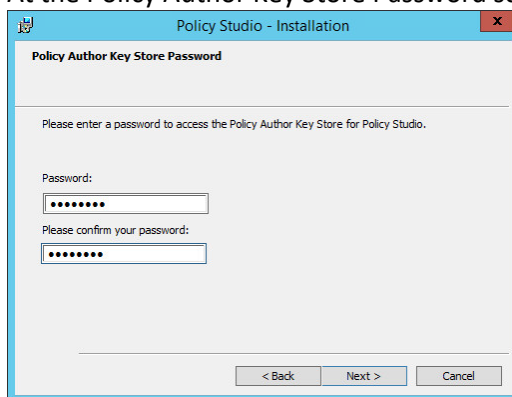


- 1151 8. At the Policy Management Server Location screen, enter the default location **localhost:8443**.

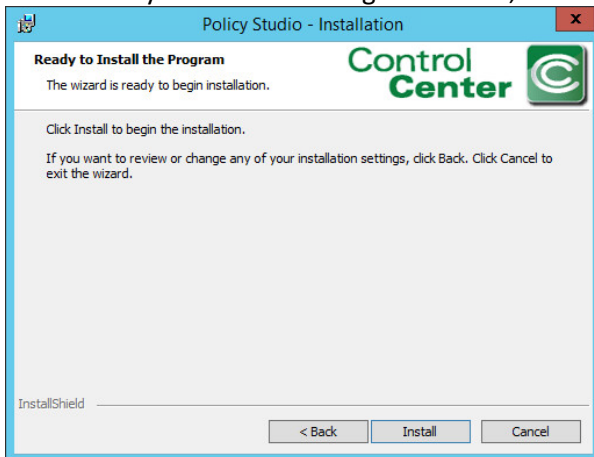


Click **Next**.

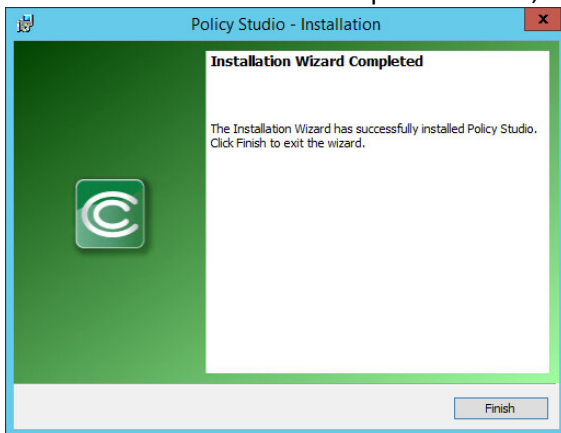
- 1153 9. At the Policy Author Key Store Password screen, enter a **Password** and click **Next**.



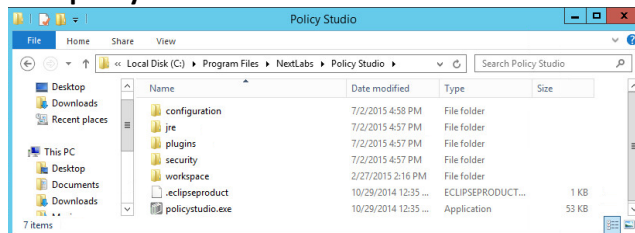
- 1157 10. At the Ready to Install the Program screen, click **Install**.



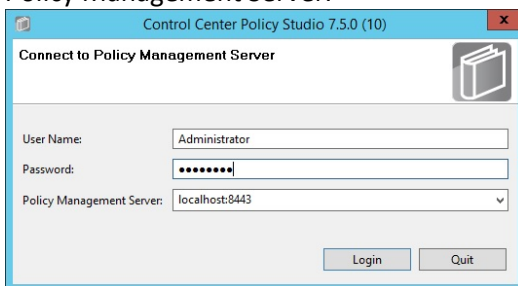
- 1158 11. At the Installation Wizard Completed screen, click **Finish**.



- 1160 12. In Windows Explorer, find and open the **polycystudio.exe** application file.
- 1161 a. Navigate to the **C:/ drive>Program Files>NextLabs>Policy Studio**.
- 1162 b. Click **polycystudio.exe**.
- 1163

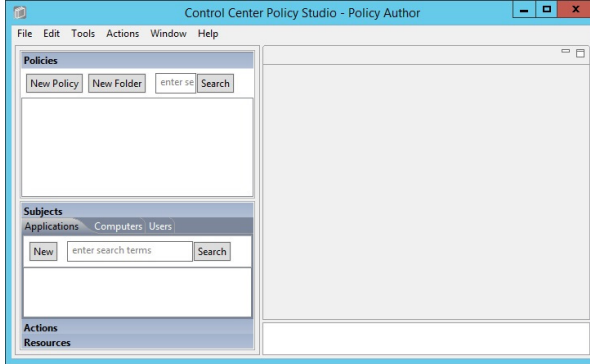


- 1164 13. In the Control Center Policy Studio window, enter a **User Name** and **Password** to connect to the
- 1165 Policy Management Server.
- 1166





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



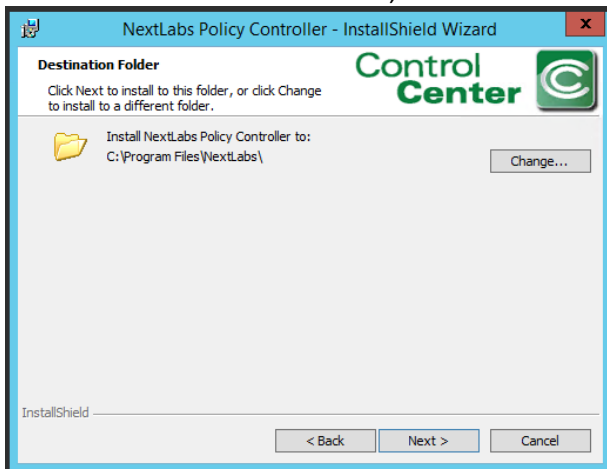
## Policy Controller 7.7

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

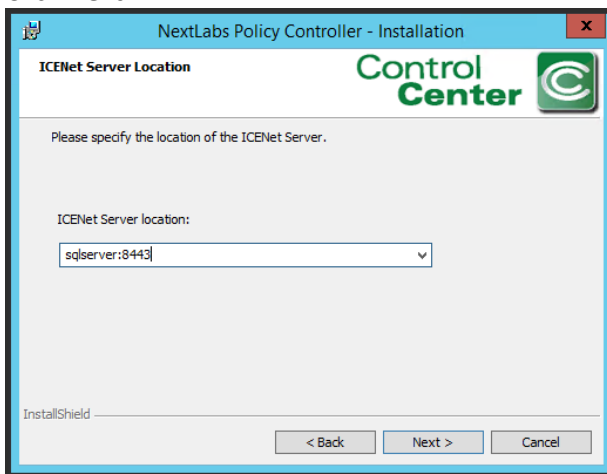
1. On the SharePoint Server, go to your desktop or other known location where the required NextLabs Policy Controller installation files are stored.
2. Extract the files from the **PolicyController-CE-64-<version>.zip** file.
3. Open the **PolicyController-CE-64-<version>** folder.
4. Click **CE-PolicyController-setup64.msi**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



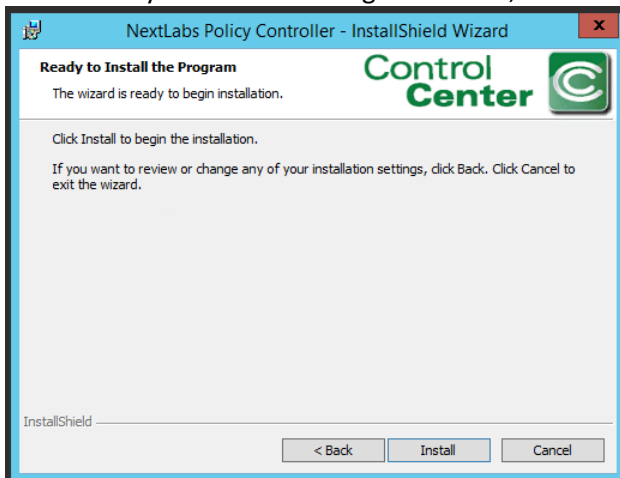
- 1184 7. At the Destination Folder screen, click **Next**.



- 1185
- 1186 8. At the ICENet Server Location screen, enter the default ICENet Server Location: sqlserver:8443.
- 1187 Click **Next**.



- 1188
- 1189 9. At the Ready to Install the Program screen, click **Install**.



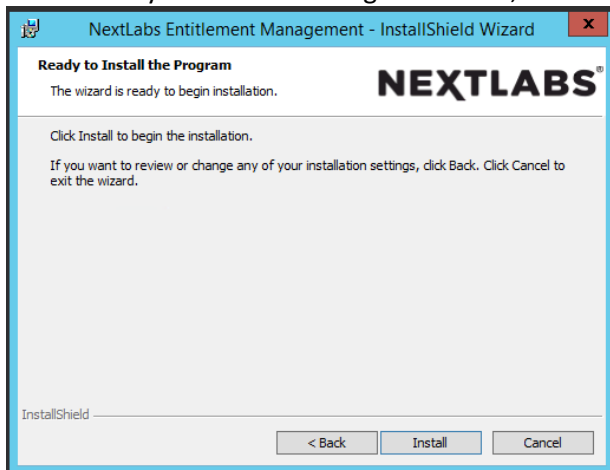
- 1190
- 1191 10. At the InstallShield Wizard Completed screen, click **Finish**.

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

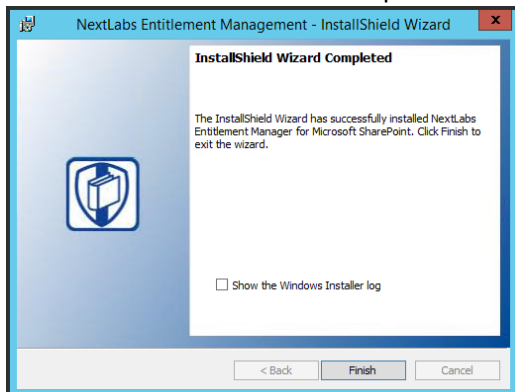
## Entitlement Manager for Microsoft SharePoint 7.6

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

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

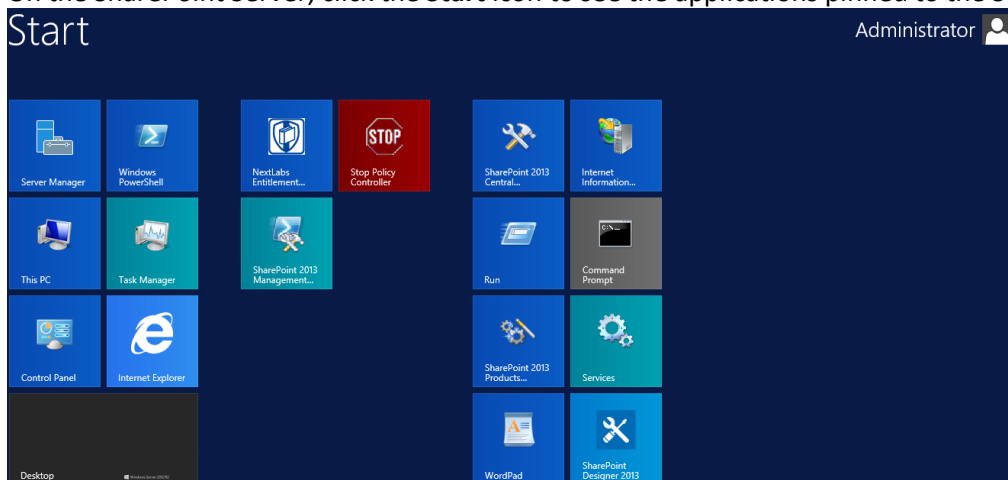


8. At the InstallShield Wizard Completed screen, click **Finish**.



9. After installing, the IIS server must be reset:
  - a. Click the Windows icon and begin typing the word **PowerShell** and open the windows PowerShell application.
  - b. From within the Windows PowerShell window, type in this command and press **Enter** to reset Internet Information Services: **iisreset**.

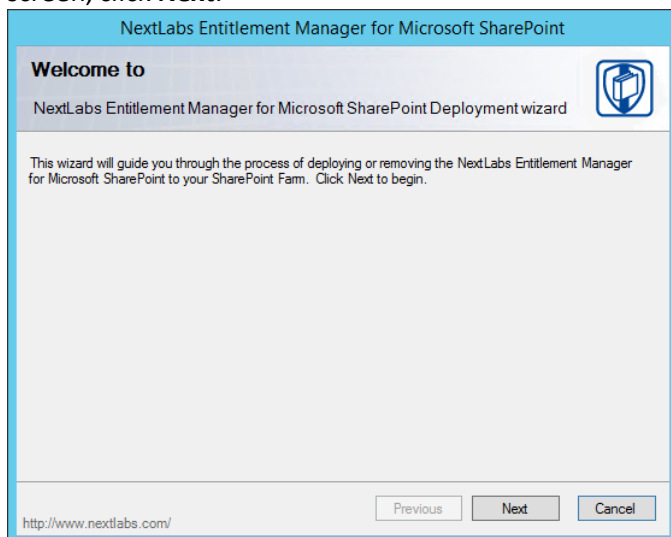
- 1216 10. On the SharePoint Server, click the **Start** icon to see the applications pinned to the **Start** menu.



- 1217  
1218 11. Click the NextLabs Entitlement Manager for SharePoint Server Deployment icon.

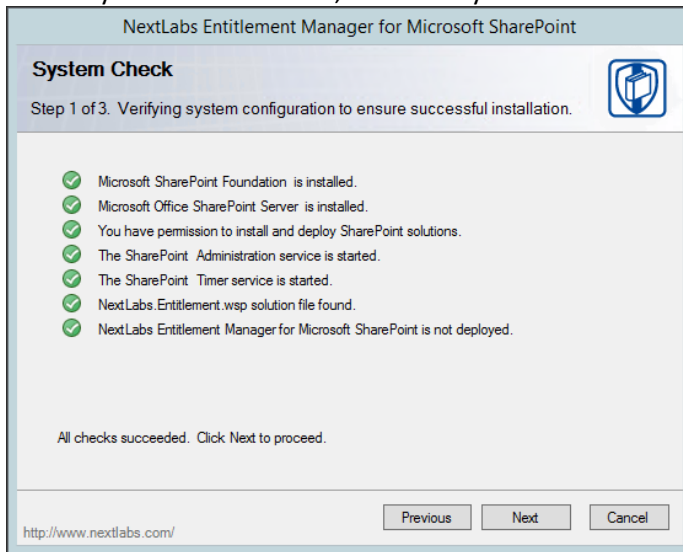
1219 This shortcut is automatically pinned during the initial installation. In case the shortcut is not created au-  
1220 tomatically, the application can be opened from File Explorer at the **location: C:\Program**  
1221 **Files\NextLabs\SharePoint Enforcer\bin\NextLabs.Entitlement.Wizard.exe**

- 1222 12. At the Welcome to NextLabs Entitlement Manager for Microsoft SharePoint Deployment wizard  
1223 screen, click **Next**.

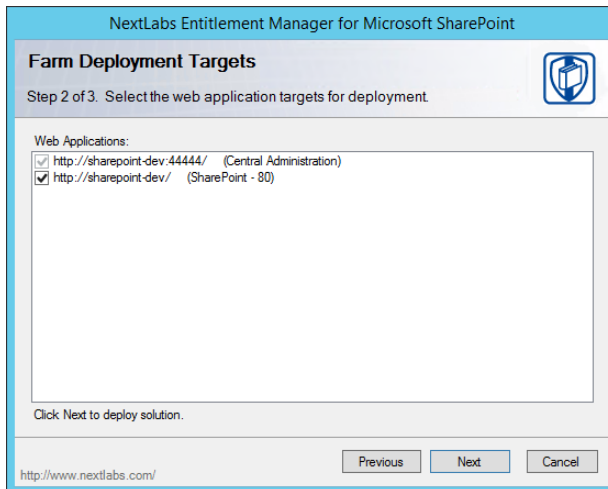


1224

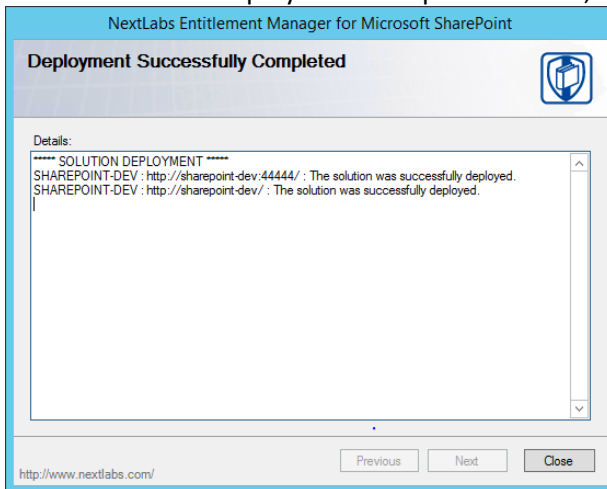
- 1225 13. At the System Check screen, after the system check is complete, click **Next**.



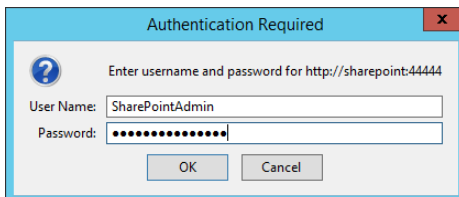
- 1226  
1227 14. At the Farm Deployment Targets screen, select the applicable web application on which to deploy.  
1228 *Note:* If only one entry is listed, i.e., **http://sharepoint:44444/Central Administration**, no web appli-  
1229 cations have been created.  
1230 15. At the Deploying Step 3 of 3 screen, click Next.



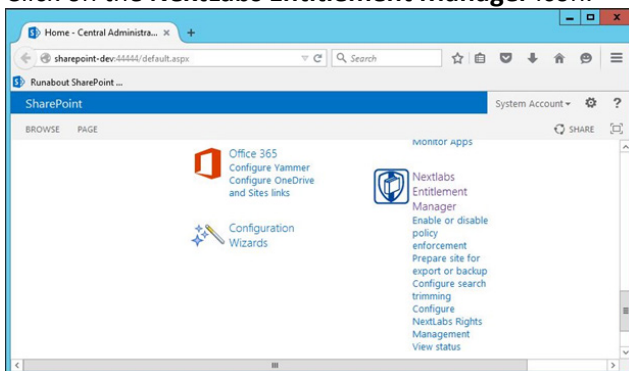
- 1231 16. At the Successful Deployment Completed screen, click **Close**.



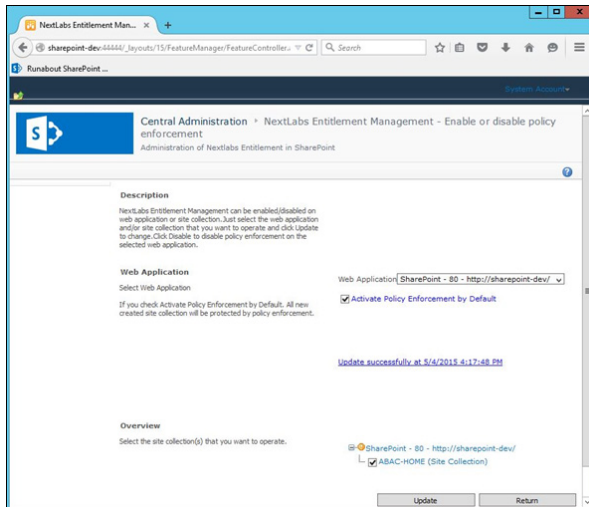
- 1232  
1233 17. Open a browser and navigate to the SharePoint Central Administration Portal. Log in with the  
1234 SharePoint Administrator account.



- 1235  
1236 18. Click on the **NextLabs Entitlement Manager** icon.



- 1237  
1238 19. In the page that opens, scroll down to verify that the correct **Web Application** is chosen and the  
1239 service is **Enabled**.



## 2.5 OpenLDAP

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

### 2.5.1 How It's Used

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

### 2.5.2 Virtual Machine Configuration

The OpenLDAP virtual machine is configured as follows:

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

#### Network Configuration (Interface 1)

IPv4 Manual  
 IPv6 Disabled  
 IP Address: 192.168.19.11  
 Netmask: 255.255.255.0  
 Gateway: 192.168.19.1  
 DNS Name Servers 192.168.19.10  
 DNS-Search Domains: acmefinancial.com

## Network Configuration (Interface 2)

IPv4 Manual

IPv6 Disabled

IP Address: 192.168.19.11

Netmask: 255.255.255.0

Gateway: 192.168.19.1

DNS Name Servers 192.168.19.10

DNS-Search Domains: acmefinancial.com

### 2.5.3 Firewall Configuration

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

```
ufw allow 636/tcp to allow
```

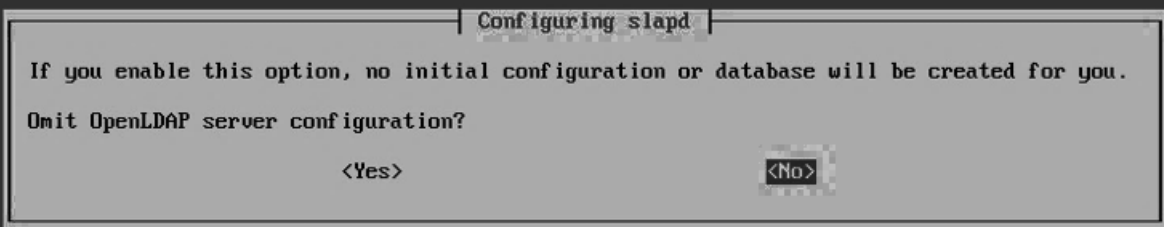
```
ufw allow 22/tcp to allow
```

```
ufw default deny incoming
```

### 2.5.4 Installation

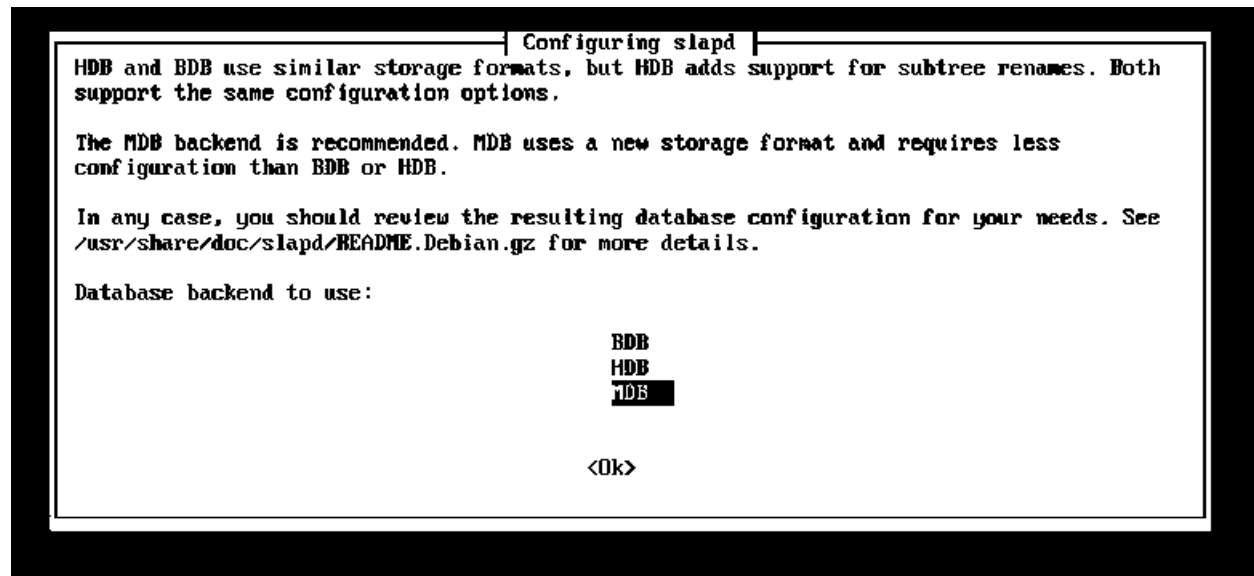
```
root@openldap:~# sudo apt-get install slapd ldap-utils
```

Package configuration



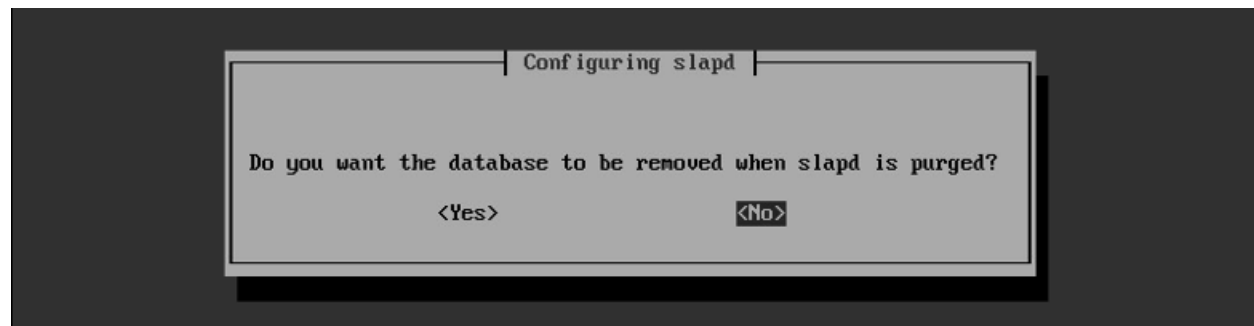
1. Select **No** and press **Enter**.
2. Enter the organizational Name on the following screen (for example, acmefinancial.com).
3. Enter the administrator password for the BaseDN (BaseDN: acmefinancial.com).





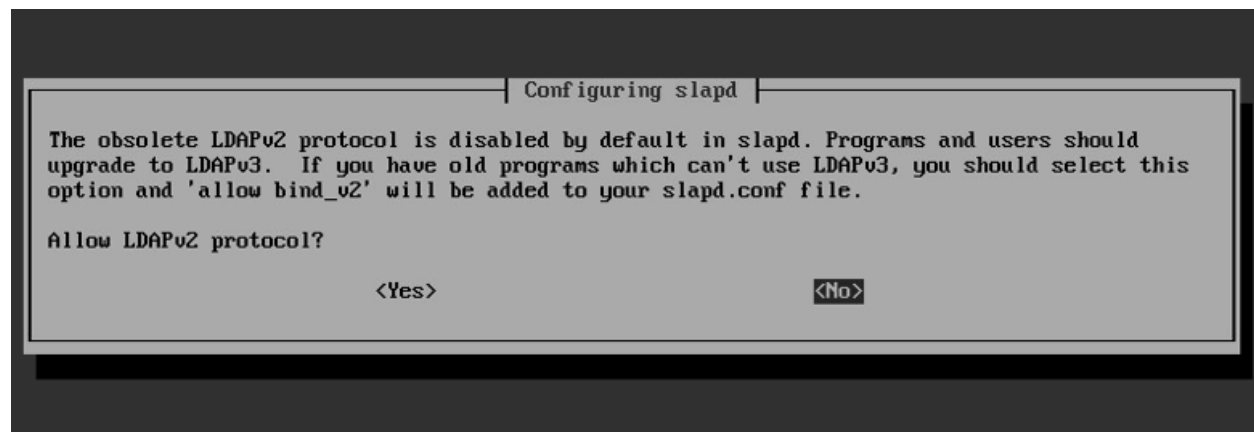
1286

1287 4. Select **MDB** as the Backend database for OpenLDAP and press **Enter**.



1288

1289 5. Select **No** and press **Enter**.



1290

1291 6. Select **No** to disable LDAPv2.

## 1292 2.5.5 Audit Configuration

1293 1. Enter `mkdir /etc/ldap/logs` at a shell prompt to create a directory that is writable by the  
1294 OpenLDAP service.

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

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

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

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

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

## 2.5.6 STARTTLS and LDAPS Configuration

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

```

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

```

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

- a. `sudo adduser openldap ssl-cert`
- b. `chgrp ssl-cert /etc/ldap/ssl/openldap_privatekey.pem`
- c. `chmod g+r /etc/ldap/ssl/openldap_privatekey.pem`
- d. `chmod o-r /etc/ssl/ldap/openldap_privatekey.pem`
- e. `chown root.ssl-cert /etc/ldap/ssl/openldap_privatekey.pem`
- f. `chown root.ssl-cert /etc/ldap/ssl/openldap_cert.pem`
- g. `chmod root.ssl-cert /etc/ldap/ssl`

6. Reconfigure slapd by running the following command

- a. `ldapmodify -Y EXTERNAL -H ldapi:/// -f /etc/ldap/ssl/certinfo.ldif`
- b. Restart slapd by running `service slapd restart`

StartTLS should now be enabled.

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

```

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

```

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

```

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

```

## 2.5.7 Formatting Audit Logs

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

## 2.5.8 Script: `/etc/ldap/logs/auditlogscript`

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

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

```
#!/usr/bin/python3
import datetime
start_index = 0
end_index = 0
timestamp = 123456789 #var to store datetime object; values are placeholders
localtime = "12345" #string var to store local time; values are placeholders
filename = "/etc/ldap/logs/auditlog.lines" #Each event in file is a line
#Open the file, parse each each line,identified char set in IF
#statement exposing the epoch_time without leading or trailing chars
with open(filename, 'r') as file_object:
    for string in file_object:
        if ";;dc" in string:
            end_index = string.find(";;dc")
            string = string.strip()
```

```

1388     newstring = string[start_index:end_index]
1389     newstring = newstring.lstrip(';')
1390     newstring = newstring.lstrip('add')
1391     newstring = newstring.lstrip('modify')
1392     newstring = newstring.lstrip('delete')
1393     newstring = newstring.lstrip('rdn')
1394     newstring = newstring.lstrip(';')
1395     epoch_time = int(newstring)      #Store epoch_time as integer
1396     #Convert epoch_time to datetime object and store in timestamp
1397     timestamp = datetime.datetime.fromtimestamp(epoch_time)
1398     #Convert value in timestamp to string and store in localtime
1399     localtime = str(timestamp)
1400     #If line is blank, do nothing, else prepend localtime to line
1401     if string.isspace():
1402         pass
1403     else:
1404         with open('/etc/ldap/logs/outlog.log','a') as outfile_object:
1405             outfile_object.write(localtime + string + '\n')

```

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

```

1407 #!/bin/bash
1408 #This script sends online status updates to splunk with enough information
1409 #such that analytics on Splunk can determine whether or not this host has
1410 #failed to send updates in a given period.
1411
1412 if ls /var/log/oldstatustime # check if file exists
1413 then
1414     prevtime=$(cat /var/log/oldstatustime) #store date in file in variable prevtime
1415 else
1416     date >/var/log/oldstatustime #else write current date to file path
1417 fi
1418 #write time hostname previous run time and online keyword to file path
1419 #in a single line separated by commas
1420 ((date && hostname && echo $prevtime && echo online)|tr -s '\n' ','|sed
1421 s'/online,/online/';echo "") >> /var/log/openldap-status-file.csv
1422 date > /var/log/oldstatustime

```

## 2.6 Radiant Logic

1424 Radiant Logic RadiantOne Virtual Directory Server (VDS) is a virtual directory that performs a federated  
1425 identity service. (Note: Radiant Logic changed their product name from RadiantOne Virtual Directory  
1426 Server (VDS) to RadiantOne Federated Identity Service (FID)).

## 2.6.1 How Its Used

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

## 2.6.2 Virtual Machine Configuration

The Radiant Logic virtual machine is configured as follows:

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

### Network Configuration (Interface 1)

IPv4 Manual  
IPv6 Disabled  
IP Address: 192.168.17.100  
Netmask: 255.255.255.0  
Gateway: 192.168.17.1  
DNS Name Servers: 192.168.17.1  
DNS-Search Domains: n/a

### Network Configuration (Interface 2)

IPv4 Manual  
IPv6 Disabled  
IP Address: 192.168.14.111  
Netmask: 255.255.255.0  
Gateway: 192.168.14.1  
DNS Name Servers 192.168.14.1  
DNS-Search Domains: n/a

## 2.6.3 Installing the Virtual Directory

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

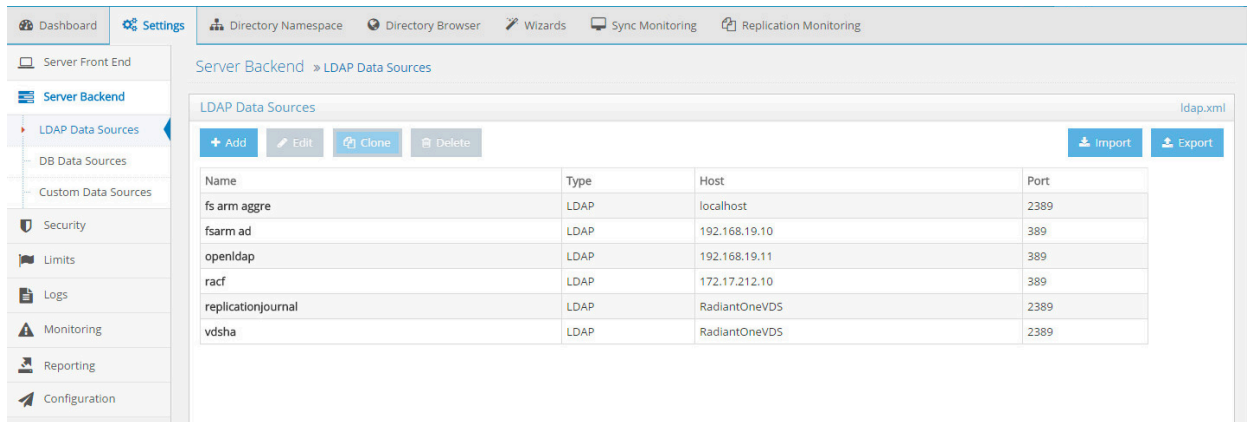
## 2.6.4 Configuring VD

Steps for configuring the VD are as follows:

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

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

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



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

**Edit LDAP Data Source**

Data Source Name: fsarm ad

Host Name: 192.168.19.10

Bind DN: Administrator@acmefinancial.com

Base DN: DC=AcmeFinancial,DC=com

Data Source Type: AD2008

Port: 389

Bind Password: [Redacted]

Use Kerberos profile: vds\_krb5

Disable Referral Chasing: [Checked]

Paged Results Control, page size: 600

Verify SSL Certificate Hostname: [Unchecked]

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

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

1476

Server Backend » LDAP Data Sources » Edit LDAP Data Source Save

**Edit LDAP Data Source**

|                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                               |                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>Data Source Name</b><br><input type="text" value="openldap"/><br><b>Host Name</b><br><input type="text" value="192.168.19.11"/><br><b>Bind DN</b><br><input type="text" value="cn=admin,dc=acmefinancial,dc=com"/><br><b>Base DN</b><br><input type="text" value="dc=acmefinancial,dc=com"/> <span>Choose</span><br><span>Test Connection</span> | <b>Data Source Type</b><br>LDAP<br><b>Port</b><br><input type="text" value="389"/> <input type="checkbox"/> SSL<br><b>Bind Password</b><br><input type="password" value="*****"/><br><input type="checkbox"/> Use Kerberos profile: vds_krb5<br><input type="checkbox"/> Disable Referral Chasing<br><input type="checkbox"/> Paged Results Control, page size: 0<br><input type="checkbox"/> Verify SSL Certificate Hostname | <b>Status</b><br>Active |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|

► Failover LDAP Servers

► Advanced

Server Backend » LDAP Data Sources » Edit LDAP Data Source Save

**Edit LDAP Data Source**

|                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                               |                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <b>Data Source Name</b><br><input type="text" value="racf"/><br><b>Host Name</b><br><input type="text" value="172.17.212.10"/><br><b>Bind DN</b><br><input type="text" value="racfid=TSNI00,profiletype=user,SYSPLEX=SYSPLEX1"/><br><b>Base DN</b><br><input type="text" value="SYSPLEX=SYSPLEX1"/> <span>Choose</span><br><span>Test Connection</span> | <b>Data Source Type</b><br>LDAP<br><b>Port</b><br><input type="text" value="389"/> <input type="checkbox"/> SSL<br><b>Bind Password</b><br><input type="password" value="*****"/><br><input type="checkbox"/> Use Kerberos profile: vds_krb5<br><input type="checkbox"/> Disable Referral Chasing<br><input type="checkbox"/> Paged Results Control, page size: 0<br><input type="checkbox"/> Verify SSL Certificate Hostname | <b>Status</b><br>Active |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|

► Failover LDAP Servers

► Advanced

1477

1478

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

1479

1480

1481

1482

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

1483

Dashboard Settings Directory Namespace Directory Browser Wizards Sync Monitoring Replication Monitoring

Proxy Backend Proxy Advanced Attributes Objects Save

Type: **LDAP Backend**  
 Naming Context: o=joinedADopenLDAP  
 Remote Base DN: DC=AcmeFinancial,DC=com Browse

**New Naming Context**

Please enter a naming context, and select the type of backend to be associated with this naming context.

Naming Context:

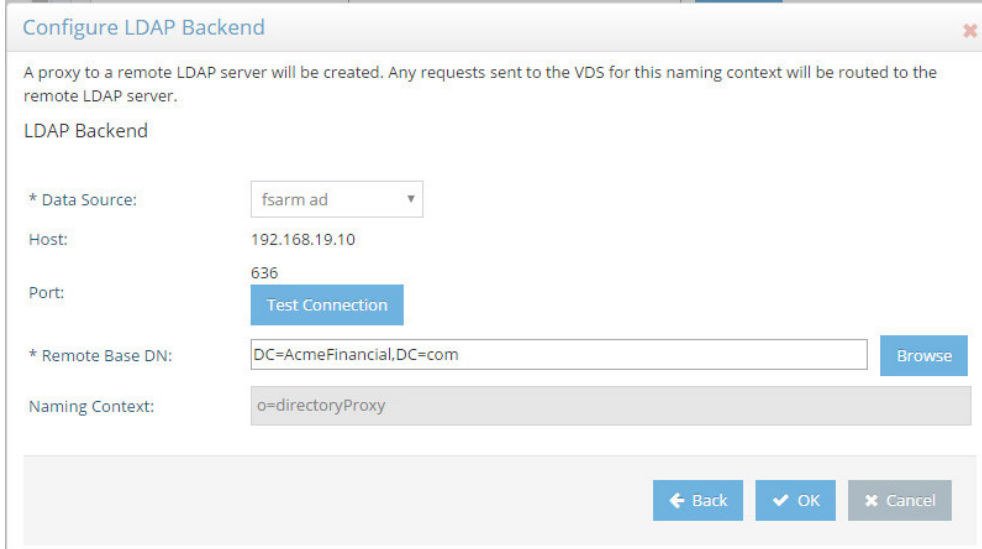
Type

- ☒ LDAP Backend
- ☐ Database Backend
- ☐ Virtual Tree
- ☐ HDAP Store
- ☐ DSML/SPML Service

Next Cancel



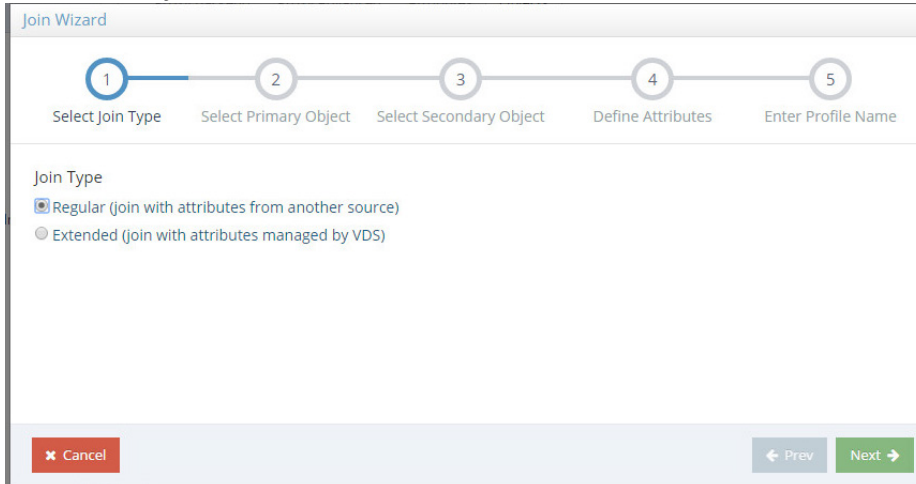
- 1484 3. Select the name of the AD backend created earlier as the **Data Source**. Select the **Remote Base**  
1485 **DN** of the domain. Select **OK**.



The 'Configure LDAP Backend' dialog box contains the following fields and controls:

- Data Source:** A dropdown menu with 'fsarm ad' selected.
- Host:** A text field containing '192.168.19.10'.
- Port:** A text field containing '636'.
- Test Connection:** A blue button.
- Remote Base DN:** A text field containing 'DC=AcmeFinancial,DC=com'.
- Browse:** A blue button.
- Naming Context:** A text field containing 'o=directoryProxy'.
- Navigation:** 'Back', 'OK', and 'Cancel' buttons at the bottom right.

- 1486 4. When the LDAP proxy is created, select the root naming context created in the left window  
1487 pane.  
1488  
1489 5. Select the **Objects** Tab. Select **New** under **Join Profiles**.



The 'Join Wizard' dialog box shows a five-step progress bar at the top: 1 (Select Join Type), 2 (Select Primary Object), 3 (Select Secondary Object), 4 (Define Attributes), and 5 (Enter Profile Name). The first step is active.

**Join Type**

- ☒ Regular (join with attributes from another source)
- ☐ Extended (join with attributes managed by VDS)

**Navigation:** 'Cancel', 'Prev', and 'Next' buttons at the bottom.

- 1490 6. Choose **Regular**. Click **Next**.  
1491

7. Select **employeeNumber** as the Join Attribute. Click **Next**. *Note:* The employee number must be unique for each user. For example, if an employee has an account in AD and OpenLDAP, the **employeeNumber** attribute should be the same in both sources for that employee.

Join Wizard

1 2 3 4 5

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

Primary Object

Base DN: o=joinedADopenLDAP

Object Class: user

\* Join Attribute: employeeNumber

Add Computed Attribute

Cancel Prev Next

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

Join Wizard

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

- 1499 9. Select **All Attributes**. Click **Next**.

Join Wizard

Progress: 1 (Select Join Type) ✓, 2 (Select Primary Object) ✓, 3 (Select Secondary Object) ✓, 4 (Define Attributes) **4**, 5 (Enter Profile Name)

Return attributes

☒ All attributes

☐ Attributes listed below:

| Actual Name      | Virtual Name |
|------------------|--------------|
| audio            |              |
| businessCategory |              |
| carLicense       |              |
| cn               |              |
| departmentNumber |              |

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

Join Wizard

Progress: 1 (Select Join Type) ✓, 2 (Select Primary Object) ✓, 3 (Select Secondary Object) ✓, 4 (Define Attributes) ✓, 5 (Enter Profile Name) **5**

Profile Name

\* Join Profile Name:

- 1502 11. Repeat Steps 5–10 to join the RACF directory using the appropriate RACF objectClass and Base
- 1503 DN.
- 1504

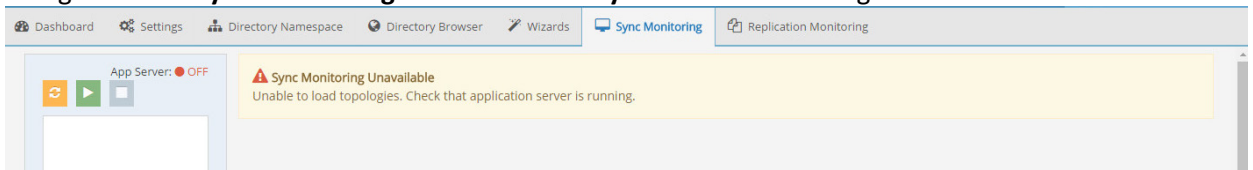
## 1505 2.6.5 Configure Logging

1506 To log changes to each directory object, you must create a cache for the proxy view created in the

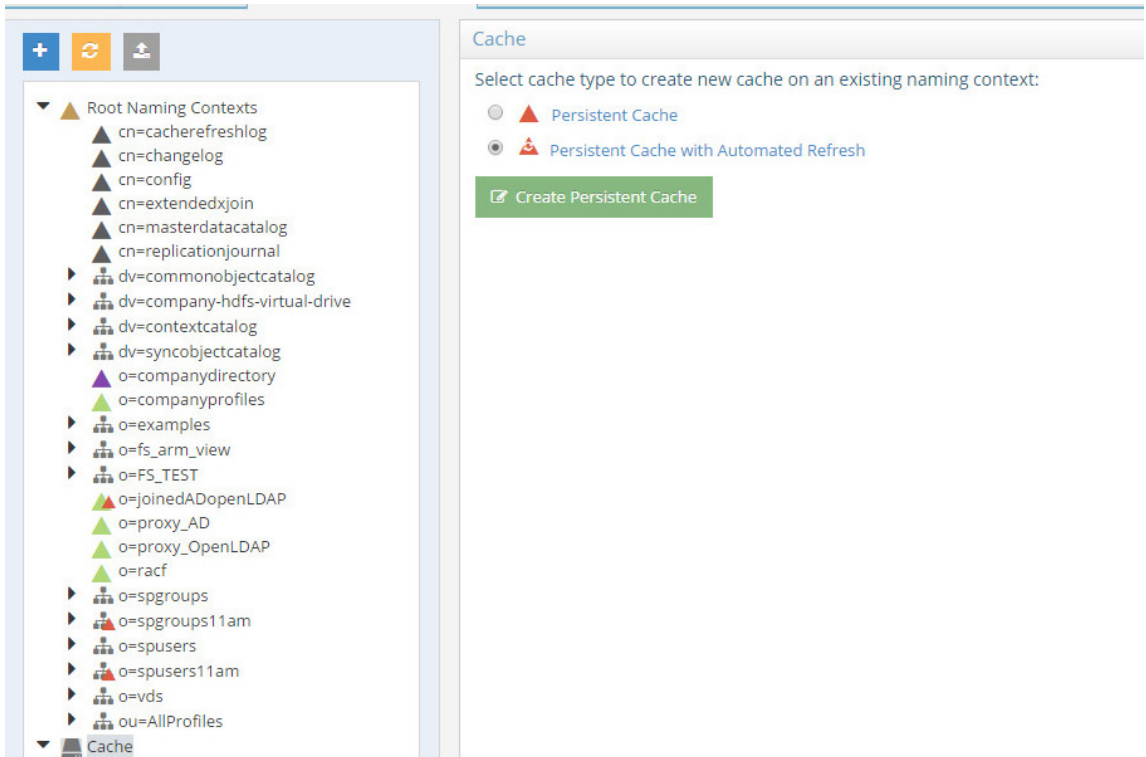
1507 previous section. To create the cache and log changes made to the backend directories, complete the

1508 following steps:

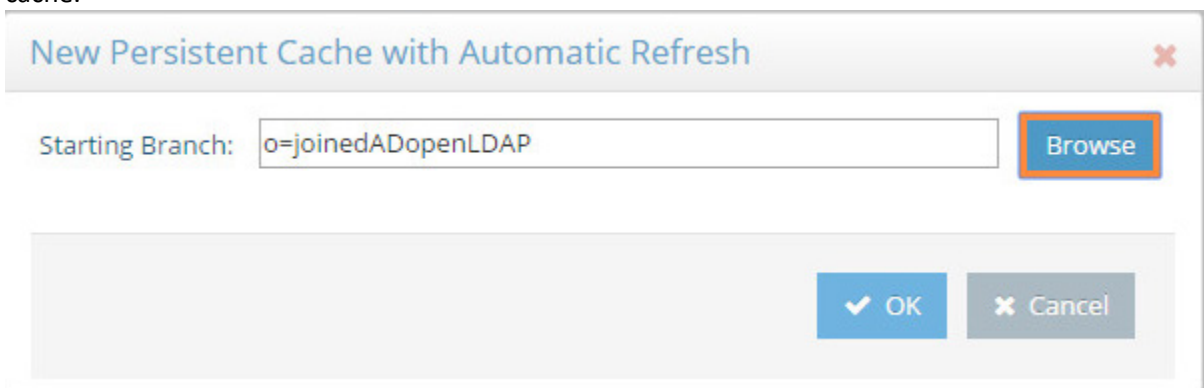
- 1509 1. Navigate to the **Sync Monitoring** tab. Press the **Play** button to start the glassfish server.



- 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

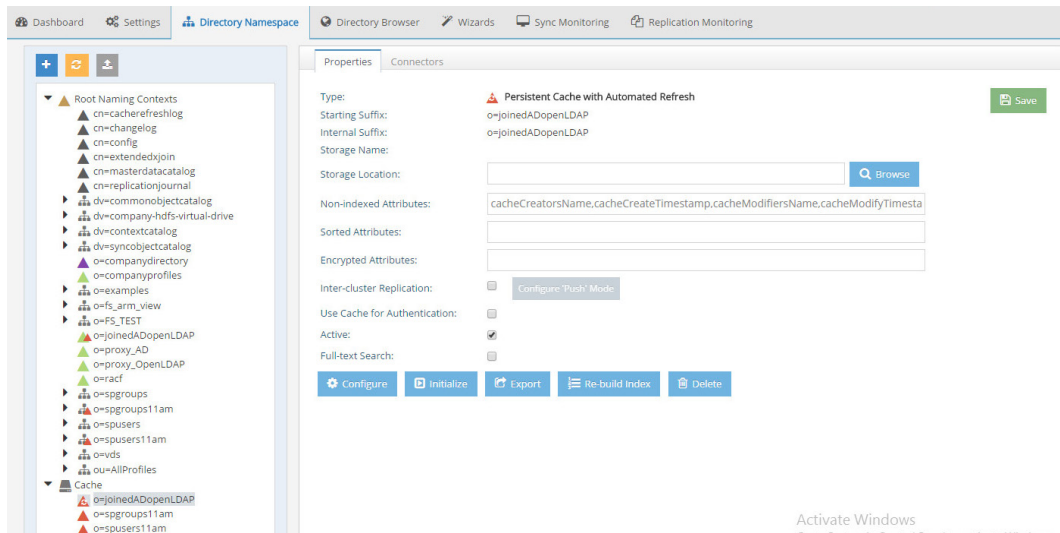


- 1513 3. Browse and select the LDAP proxy created in the previous section. Select **OK**. The VD creates the  
 1514 cache.  
 1515

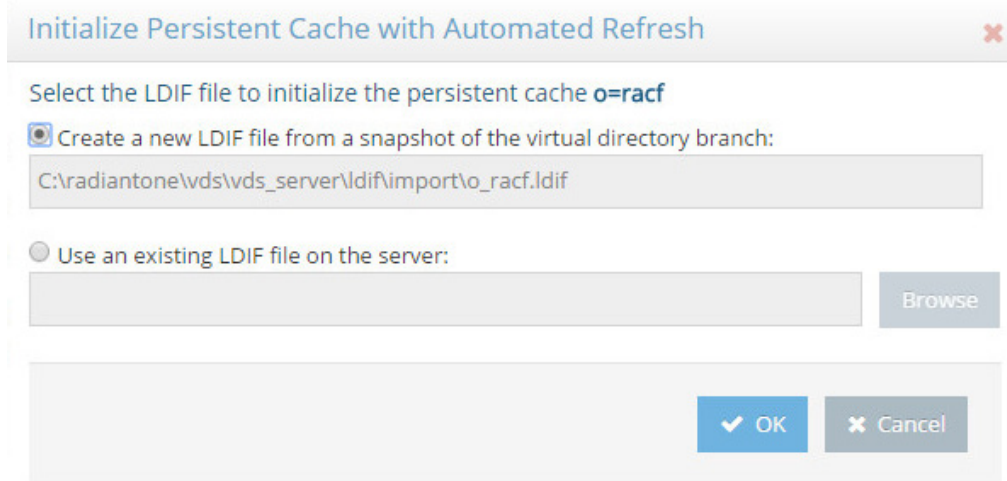


1516

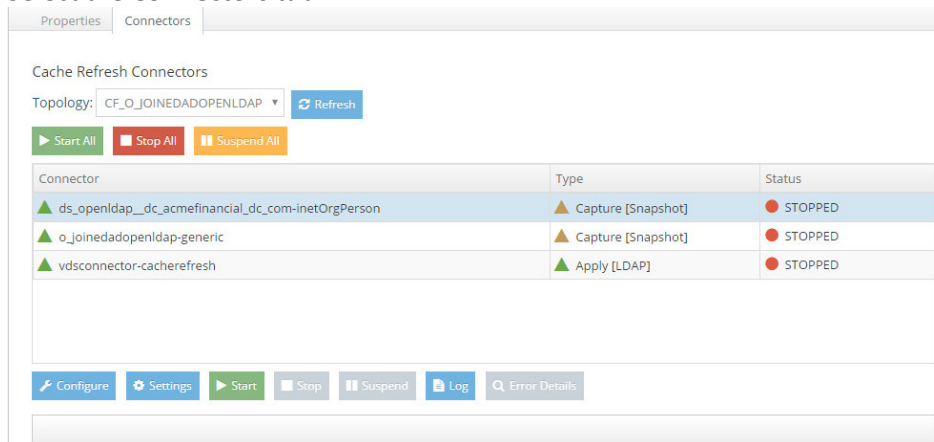
- 1517 4. Select the created cache from the lower left window. Click **Initialize** to make the cache active.



- 1518 5. Select **Create a new LDIF file from a snapshot of the virtual directory branch**. Click **OK**. This step  
 1519 may take a while depending on the number of accounts in the backend directories.  
 1520

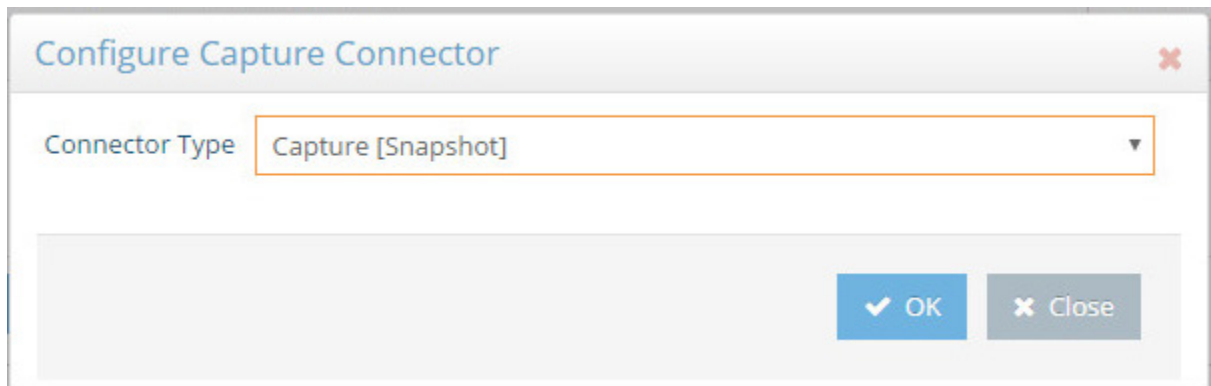


- 1521 6. Once complete, **Save** the settings.  
 1522  
 1523 7. Select the **Connectors** tab.

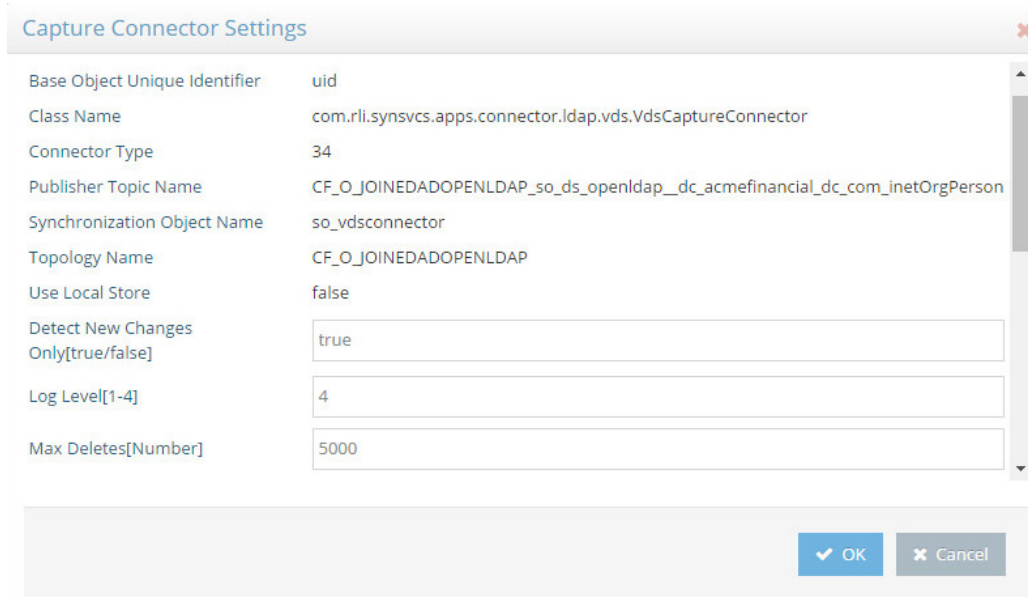


1524

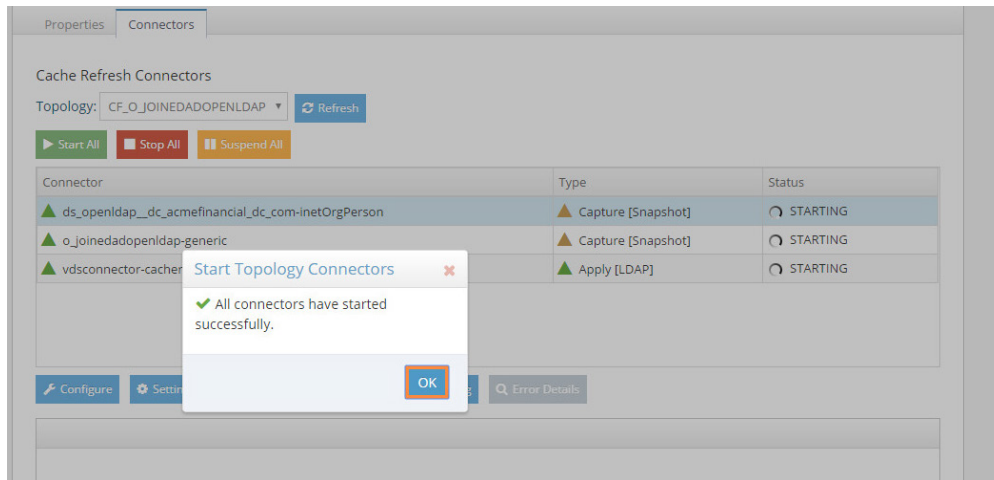
8. There should be a connector for each backend directory and one for the connector itself. Highlight the first connector. Select **Configure**. Change the connector type to "Capture [Snapshot]." Click **OK**. Repeat this step for each connector except the "vdsconnector-cacherefresh."



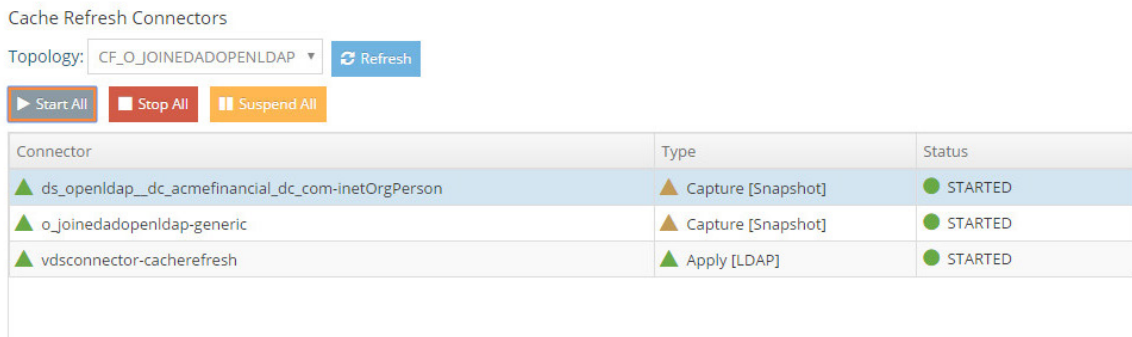
9. Back at the **Connectors** tab, highlight the first connector. Select **Settings**. Change the log level to the number 4. Click **OK**. Repeat this step for each connector except the "vdsconnector-cacherefresh."



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



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

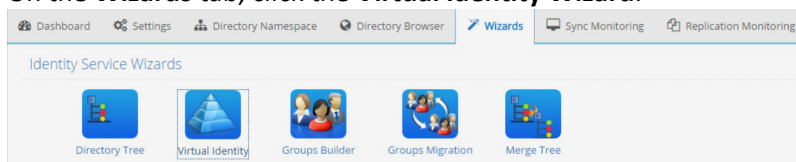


## 2.6.6 Configure Views for SharePoint

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

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

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



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



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

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

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



Projects Identities Mapping Authentication Extension Attribute Precedence Deployment

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

Identities  
Select Identity Objects  
Select Virtual Identity Object Class  
Identity Overlap

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

☒ YES  
☐ NO


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

**Define correlation key**

RDN Name of your identities:

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

| Identity object                | Correlation key                                       |
|--------------------------------|-------------------------------------------------------|
| o_proxy_ad.user                | <input checked="" type="checkbox"/> cn=employeeNumber |
| o_proxy_openldap.inetOrgPerson | <input checked="" type="checkbox"/> cn=employeeNumber |

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

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

Expression:

**ATTRIBUTES** **FUNCTIONS** **CONSTANT** **VALIDATE**

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

**Define correlation key**

RDN Name of your identities:

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

| Identity object                | Correlation key                                       |
|--------------------------------|-------------------------------------------------------|
| o_proxy_ad.user                | <input checked="" type="checkbox"/> cn=employeeNumber |
| o_proxy_openldap.inetOrgPerson | <input checked="" type="checkbox"/> cn=employeeNumber |

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

**Define Attribute Mappings**

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

Identity Object:

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              |
| c                             |        |                               |

**BACK** **NEXT**

- 1581 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**

- 1582 15. Select **Next** once the source attributes are mapped to the Virtual identity attribute.
- 1583 16. Select the **uid** attribute as the identification attribute for user. The **uid** attribute contains the
- 1584 value that users will log in to SharePoint with. Select **Next**.
- 1585

**Identification**

Select how you would like to identify the users.

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

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

- 1586 17. Enable both AD and OpenLDAP for credential checking. Give ADprecedence in the bind order.
- 1587 Click **Next**.
- 1588

**Credential checking strategy** ?

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

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

- 1589 18. Do not select **Join Objects**. Click **Next**.
- 1590

**Select Join Objects**

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

Schema:  +

inetOrgPerson  
person  
user

➔

×

?

Selected Join Objects:

Starting point: DC=AcmeFinancial,DC=com

◀ BACK      NEXT ▶

- 1591  
1592  
1593
19. You can set each attribute precedence for any attributes that have mappings from multiple objects. Select the employeeNumber attribute. Click **PRECEDENCE**.

**Virtual Identity Attributes**

The following attributes will appear in your virtual identity.

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

**PRECEDENCE**

Attributes

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

- 1594  
1595
20. Give AD the highest priority. Click **O**

#### Attribute mappings:

Virtual identity attribute: **employeeNumber**

| Identity Origin                | Attribute from Origin | Priority      |
|--------------------------------|-----------------------|---------------|
| o_proxy_ad.user                | employeeNumber        | 1 - HIGHEST ▼ |
| o_proxy_openldap.inetOrgPerson | employeeNumber        | 3 - NORMAL ▼  |

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

OK

CANCEL

- 1596  
1597  
1598
21. Click **Next**.
22. Name the naming context. For example, cn=spusers. Click **Next**.

**Mount Point**

☒ Mount under a new Naming Context

Naming Context:

?

- 1599  
1600
23. Select **Yes, I want a Periodic Cache Refresh**. Click **Next**.

**Define a cache** ?

Do you want to use a cache?

☐ NO

☒ YES, I want a Periodic Cache Refresh

☐ YES, I want a Real Time Cache Refresh

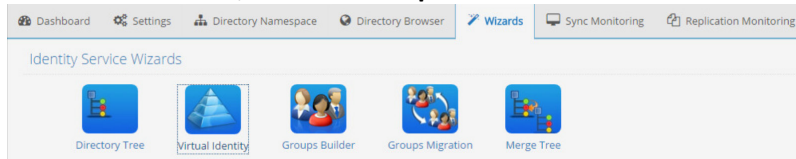
If you want to use your own storage, do not set up the cache in the Wizard (choose NO), and configure your cache in the Control Panel (Directory Namespace tab) once the Wizard is complete.

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

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

Follow these steps to configure the groups for SharePoint:

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



2. Click **Next**.

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

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

**Group configuration** ?

What object class should represent your groups?

group (Active Directory)

Select how groups will be created:

☒ User-Defined: Members can be assigned explicitly and/or dynamically by performing an LDAP search.

☐ Auto-Generated: Group names will be auto generated based on the specified user attribute and members will be assigned accordingly.

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

**Enter a name for your group:**

Name:

ITinfr

6. Repeat Step 5. Name the group Operations.

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

**Define your groups** ?

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

**NEW GROUP** **DELETE GROUP**

| Group                                   | Membership                                                                                                                                  |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="radio"/> ITinfr | <b>Manage Individual Members</b> <b>Define Dynamic Members</b><br>o=spusers11am; SUBTREE; (& (objectclass=person) (actualdn=*,OU=ITinfr,*)) |
| <input type="radio"/> Operations        |                                                                                                                                             |

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

1620 **Sub-Tree.** Click **Next**.

Define who belongs to the group 'ITinfr'

Base DN:

o=spusers11am

CHOOSE

Filter:

(& (objectclass=person) (actualdn=\*,OU=ITinfr,\*))

☐ One Level ☒ Sub-Tree

PREVIEW

1621 9. Repeat Steps 7 and 8 with the following filter: (& (objectclass=person) (actualdn=\*,OU=Operations,\*)) .

1622 10. Click **Next**.

Define your groups

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

NEW GROUP DELETE GROUP

| Group      | Membership                                                                    |
|------------|-------------------------------------------------------------------------------|
| ITinfr     |                                                                               |
| Operations | o=spusers11am; SUBTREE: (& (objectclass=person) (actualdn=*,OU=Operations,*)) |

Manage Individual Members Define Dynamic Members

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

Mount Point

☒ Mount under a new Naming Context

Naming Context :

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

Define a cache

Do you want to use a cache?

☐ NO

☒ YES, I want a Periodic Cache Refresh

☐ YES, I want a Real Time Cache Refresh

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

1629 13. Define the refresh interval. Click **Next**.

1630 14. Click **Initialize Cache Now**. Click **Finish**.

## 1632 2.6.7 Scripts

1633 Two PowerShell scripts are scheduled to run on regular intervals on RadiantOne VDS server. The goal of  
 1634 these scripts is to determine if the virtual directory server (RadiantOne VDS) and the RACF directory  
 1635 server are online or offline. The first script determines if RadiantOne VDS is online or offline and writes  
 1636 the corresponding status message to a local file being monitored by Splunk. The second script, which  
 1637 also runs on the RadiantOne VDS server, determines if the Vanguard RACF directory is reachable and  
 1638 writes corresponding offline or online messages to a local file also being monitored by Splunk.

## 2.6.8 Script: RadiantOnlineStatus.ps1

```

1639 #This script checks determines if this server is online or offline
1640 #If gateway route exists and VDS server is running, the script will
1641 #output the current time, hostname, status and previous time (last
1642 #time it wrote to output file)
1643 #Check if gateway route exists and if the VDS service is running
1644 if ((Get-Netroute 0.0.0.0/0) -And (Get-Process vdsserver))
1645 {
1646     #Store date in PrevTime variable
1647     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1648     #Check if prevtime-file.txt exists
1649     if (ls C:\scripts\Radiant\prevtime-file.txt)
1650     {
1651         #Place the contents of prevtime-file.txt in the PrevTime variable
1652         $PrevTime=Get-Content C:\scripts\Radiant\prevtime-file.txt
1653     }
1654     #Place the current date in CurrentTime
1655     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1656     #Overwrite the contents of prevtime-file.txt with the current date
1657     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy" > C:\scripts\Radiant\prevtime-
1658     file.txt
1659     $HostVar = hostname
1660     $Status = 'online'
1661     #Add the contents of the variables CurrentTime, HostVar, Status, PrevTime to
1662     Radiant-Status-Output.csv
1663     Add-Content C:\scripts\Radiant\Radiant-Status-Output.csv
1664     $CurrentTime','$HostVar','$Status','$PrevTime
1665 }
1666 else
1667 {
1668     #Store date in PrevTime variable
1669     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1670     #Check if prevtime-file.txt exists
1671     if (ls C:\scripts\Radiant\prevtime-file.txt)
1672     {
1673         #Place the contents of prevtime-file.txt in the PrevTime variable
1674         $PrevTime=Get-Content C:\scripts\Radiant\prevtime-file.txt
1675     }
1676     #Place the current date in CurrentTime
1677     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1678     #Overwrite the contents of prevtime-file.txt with the current date
1679     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy" > C:\scripts\Radiant\prevtime-
1680     file.txt
1681     $HostVar = hostname
1682     $Status = 'offline'

```



```

1679     Add-Content C:\scripts\Radiant\Radiant-Status-Output.csv
1680 $CurrentTime','$HostVar','$Status','$PrevTime
1681 }

```

## 1682 2.6.9 Script: VanguardOnlineStatus.ps1

```

1683 #Script checks if the RACF mainframe is online and outputs status messages to file
1684
1685 #Check if the RACF mainframe is reachable with pings
1686
1687 if (ping -n 3 172.17.212.10 | select-string "Reply from 172.17.212.10")
1688 {
1689     #Store date in PrevTime variable
1690     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1691     #Check if prevtime-file.txt exists
1692     if (ls C:\scripts\Vanguard\prevtime-file.txt)
1693     {
1694         #Place the contents of prevtime-file.txt in the PrevTime variable
1695         $PrevTime=Get-Content C:\scripts\Vanguard\prevtime-file.txt
1696     }
1697     #Place the current date in CurrentTime
1698     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
1699     #Overwrite the contents of prevtime-file.txt with the current date
1700     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\Vanguard\prevtime-
1701 file.txt
1702     $HostVar = "VanguardMainframe.acmefinancial.com"
1703     $Status = 'online'
1704     Add-Content C:\scripts\Vanguard\VanguardServer-Output.csv
1705 $CurrentTime','$HostVar','$Status','$PrevTime
1706 }
1707 else
1708 {
1709     $PrevTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyyy"
1710     if (ls C:\scripts\Vanguard\prevtime-file.txt)
1711     {
1712         $PrevTime=Get-Content C:\scripts\Vanguard\prevtime-file.txt
1713     }
1714     $CurrentTime = Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy"
1715     Get-Date -format "ddd MMM dd HH:mm:ss \EST yyy" > C:\scripts\Vanguard\prevtime-
1716 file.txt
1717     $HostVar = "VanguardMainframe.acmefinancial.com"
1718     $Status = 'offline'

```

```

1719     Add-Content C:\scripts\Vanguard\VanguardServer-Output.csv
1720     $CurrentTime', '$HostVar', '$Status', '$PrevTime
1721 }

```

## 1722 2.6.10 LDAPS Configuration

1723 RadiantOne VDS virtual directory service connects to the Active Directory, OpenLDAP, and RACF  
 1724 backend directory servers and takes snapshots of the directory contents. Configuring LDAPS ensures  
 1725 that this process is encrypted with SSL. To use LDAPS to make these connections, follow these steps:

- 1726 1. Copy the certificates of the backend directories to the RadiantOne VDS virtual directory server.
- 1727 2. Import each certificate into the client trust store by opening the **Main Control Panel**.
- 1728 3. Click **Settings** tab > **Security** section > **Client Certificate Trust Store**.
- 1729 4. The certificates will be dynamically loaded into the Client Certificate Trust Store.
- 1730 5. Configure the backend connections to use LDAPS by going to the **Settings** tab.
- 1731 6. Click **Server Backend** > **LDAP Data Sources** > **Edit LDAP Data Source**.
- 1732 7. Check the **SSL** box and type **636** into the **Port** text box.

## 1733 2.7 SharePoint

1734 SharePoint is a web-based, collaborative platform. SharePoint is primarily used as a document  
 1735 management and storage system. It also supports workflow and applications.

### 1736 2.7.1 How It's Used

1737 SharePoint 2013 is used as the web application to demonstrate the capability of the Access Rights  
 1738 Management example solution.

### 1739 2.7.2 Virtual Machine Configuration

1740 The SharePoint virtual machine is configured as follows:

- 1741 ■ Ubuntu Linux 16.04 LTS
- 1742 ■ 4 CPU cores
- 1743 ■ 32GB of RAM
- 1744 ■ 2 NICs
- 1745 ■ 120GB of storage

#### 1746 Network Configuration (Interface 1)

1747 IPv4 Manual  
 1748 IPv6 Disabled  
 1749 IP Address: 192.168.17.113  
 1750 Netmask: 255.255.255.0  
 1751 Gateway: 192.168.17.1  
 1752 DNS Name Servers: 192.168.19.10  
 1753 DNS-Search Domains: acmefinancial.com

### 1754 2.7.3 Prerequisites

1755 See the Microsoft [online](#) documentation for hardware and software prerequisites.

### 1756 2.7.4 Installing SharePoint 2013

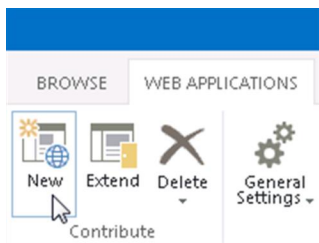


1. Installing SQL Server 2012: On the server where SharePoint 2013 is going to be installed, follow the steps from this link to install SQL Server 2012: [https://technet.microsoft.com/en-us/library/ms143219\(v=sql.110\).aspx](https://technet.microsoft.com/en-us/library/ms143219(v=sql.110).aspx)
2. Installing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

## 2.7.5 Configuring SharePoint

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

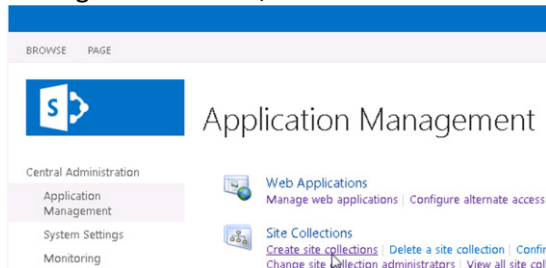
1. Open the SharePoint Central Administration Console, log in with your admin user, and click **Application Management**.
2. Below the **Web Applications** section, click on **Manage Web Applications**.



3. Click the **New** button.
  4. You can choose to create a new IIS website and set a unique port.
- Typically, you should accept the default path.
5. In the Security Configuration section, you can leave the default options (Allow Anonymous=No, Use SSL=No).
  6. In the Claims Authentication Types section, check the option to **Enable Forms Based Authentication (FBA)**.

7. Enter a unique name for the ASP.NET Membership provider name and ASP.NET Role manager name.

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



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

1799

**Create Site Collection**

**Web Application**  
Select a web application.  
To create a new web application go to [New Web Application](#) page.  
Web Application: <http://demo-empty.sharepoint.com:48888>

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

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

**Template Selection**  
Select experience version:  
2013  
Select a template:  
Collaboration Enterprise Publishing Custom  
**Team Site**  
Blog  
Developer Site  
Project Site  
Community Site

1800

1801

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

**Template Selection**

Select experience version:  
2013  
Select a template:  
Collaboration Enterprise Publishing Custom  
**Team Site**  
Blog  
Developer Site  
Project Site  
Community Site

A place to work together with a group of people.

**Primary Site Collection Administrator**  
Specify the administrator for this site collection. Only one user login can be provided; security groups are not supported.  
User name:

**Secondary Site Collection Administrator**  
Optionally specify a secondary site collection administrator. Only one user login can be provided; security groups are not supported.  
User name:

**Quota Template**  
Select a predefined quota template to limit resources used for this site collection.  
To add a new quota template, go to the [Manage Quota Templates](#) page.  
Select a quota template:  
No Quota  
Storage limit:  
Number of invited users:

1802

## 1803 2.7.6 Web Configs

1804 Three web config files must be edited to complete the integration with Radiant Logic.

1805 SharePoint STS web config file is located at C:\Program Files\Common Files\Microsoft Shared\Web  
1806 Server Extensions\15\WebServices\SecurityToken.

1807 The web.config file has a default membership provider and a default role provider. Do not change them.  
1808 The names of the new membership provider and role manager that get added into the web.config file  
1809 must match the names set in the Forms Based configuration for the web application.

1810 Modify the file to include the following xml code in the <system.web> section.

```
1811 <system.web>
1812 <membership defaultProvider="i">
1813 <providers>
1814 <clear/>
1815 <add name="i"
1816 type="Microsoft.Sharepoint.Administration.Claims.SPClaimsAuthMembershipProvider,
1817 Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
1818 PublicKeyToken=71e9bce11e9429c" />
```

## DRAFT

```
1819 <add name="VDSMembership"
1820 type="Microsoft.Office.Server.Security.LdapMembershipProvider,
1821 Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
1822 PublicKeyToken=71e9bce111e9429c"
1823     server="192.168.14.111"
1824     port="2389"
1825     useSSL="false"
1826     connectionUsername="cn=Directory Manager"
1827     connectionPassword="Fsarm@nccoe1"
1828     useDNAttribute="false"
1829     userDNAttribute="distinguishedName"
1830     userNameAttribute="uid"
1831     userContainer="o=spusers11am"
1832     userObjectClass="user"
1833     userFilter="(ObjectClass=user) "
1834     scope="Subtree"
1835     otherRequiredUserAttributes="sn,givenname,cn,employeeNumber"/>
1836 </providers>
1837 </membership>
1838 <roleManager defaultProvider="c" enabled="true" cacheRolesInCookie="false" >
1839 <providers>
1840 <clear/>
1841 <add name="c"
1842 type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthRoleProvider,
1843 Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
1844 PublicKeyToken=71e9bce111e9429c" />
1845 <add name="VDSRole"
1846 type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
1847 Version=15.0.0.0, Culture=neutral, PublicKeyToken=71e9bce111e9429c"
1848     server="192.168.14.111"
1849     port="2389"
1850     useSSL="false"
1851     groupContainer="o=spgroups11am"
1852     groupNameAttribute="cn"
1853     groupNameAlternateSearchAttribute="cn"
1854     groupMemberAttribute="member"
1855     userNameAttribute="uid"
1856     useUserDNAttribute="false"
1857     userContainer="o=spusers11am"
1858     dnAttribute="distinguishedName"
1859     groupFilter="(ObjectClass=group) "
1860     userFilter="(ObjectClass=user) "
```

## DRAFT

```
1861         scope="Subtree" />
1862     </providers>
1863 </roleManager>
1864 </system.web>

1865 SharePoint Central Admin web config file is located at C:\inetpub\wwwroot\wss\VirtualDirectories\<port
1866 the central admin is on>.

1867 There is a default membership provider and a default role provider in the web.config file. Do not change
1868 them. The names of the new membership provider and role manager that get added into the web.config
1869 file must match the names set in the Forms Based configuration for the web application.

1870 Modify the file to include the following xml code in the <system.web> section:

1871 <membership defaultProvider="i">
1872     <providers>
1873         <clear />
1874         <add name="i"
1875             type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthMembershipProvider,
1876             Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
1877             PublicKeyToken=71e9bce111e9429c" />
1878         <add name="VDSMembership"
1879             type="Microsoft.Office.Server.Security.LdapMembershipProvider,
1880             Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
1881             PublicKeyToken=71e9bce111e9429c"
1882                 server="192.168.14.111"
1883                 port="2389"
1884                 useSSL="false"
1885                 connectionUsername="cn=Directory Manager"
1886                 connectionPassword="Fsarm@nccoe1"
1887                 useDNAttribute="false"
1888                 userDNAttribute="distinguishedName"
1889                 userNameAttribute="uid"
1890                 userContainer="o=spusers1lam"
1891                 userObjectClass="user"
1892                 userFilter="(ObjectClass=user) "
1893                 scope="Subtree"
1894                 otherRequiredUserAttributes="sn,givenname,cn,employeeNumber"/>
1895     </providers>
1896 </membership>
1897 <roleManager defaultProvider="c" enabled="true" cacheRolesInCookie="false">
1898     <providers>
1899         <clear />
1900         <add name="c"
1901             type="Microsoft.SharePoint.Administration.Claims.SPClaimsAuthRoleProvider,
1902             Microsoft.SharePoint, Version=15.0.0.0, Culture=neutral,
1903             PublicKeyToken=71e9bce111e9429c" />
```

## DRAFT

```
1904 <add name="VDSRole"
1905 type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
1906 Version=15.0.0.0, Culture=neutral, PublicKeyToken=71e9bce11e9429c"
1907     server="192.168.14.111"
1908     port="2389"
1909     useSSL="false"
1910     groupContainer="o=spgroups11am"
1911     groupNameAttribute="cn"
1912     groupNameAlternateSearchAttribute="cn"
1913     groupMemberAttribute="member"
1914     userNameAttribute="uid"
1915     useUserDNAttribute="false"
1916     userContainer="o=spusers11am"
1917     cacheDurationInMinutes="0"
1918     dnAttribute="distinguishedName"
1919     groupFilter="(ObjectClass=group) "
1920     userFilter="(ObjectClass=user) "
1921     scope="Subtree" />
1922 </providers>
1923 </roleManager>
```

1924 SharePoint Web Application web config is located at *C:\inetpub\wwwroot\wss\VirtualDirectories\<port*  
1925 *the application is on>*.

1926 There is a default membership provider and a default role provider in the web.config file. Do not change  
1927 them. The names of the new membership provider and role manager that get added into the web.config  
1928 file must match the names set in the Forms Based configuration for the web application.

1929 Modify the file to include the following xml code in the <system.web> section:

```
1930 <roleManager enabled="true" defaultProvider="AspNetWindowsTokenRoleProvider"
1931 <providers>
1932 <add name="VDSRole"
1933 type="Microsoft.Office.Server.Security.LdapRoleProvider, Microsoft.Office.Server,
1934 Version=15.0.0.0, Culture=neutral,
1935 PublicKeyToken=71e9bce11e9429c"
1936     server="192.168.14.111"
1937     port="2389"
1938     useSSL="false"
1939     groupContainer="o=spgroups11am"
1940     groupNameAttribute="cn"
1941     groupNameAlternateSearchAttribute="cn"
1942     groupMemberAttribute="member"
1943     userNameAttribute="uid"
```

## DRAFT

```
1944         dnAttribute="distinguishedName"
1945         groupFilter="(ObjectClass=group) "
1946         userFilter="(ObjectClass=person) "
1947         scope="Subtree" />
1948     </providers>
1949 </roleManager>
1950 <membership>
1951     <providers>
1952     <add name="VDSMembership"
1953         type="Microsoft.Office.Server.Security.LdapMembershipProvider,
1954         Microsoft.Office.Server, Version=15.0.0.0, Culture=neutral,
1955         PublicKeyToken=71e9bce11e9429c"
1956         server="192.168.14.111"
1957         port="2389"
1958         useSSL="false"
1959         connectionUsername="cn=Directory Manager"
1960         connectionPassword="Fsarm@nccoe1"
1961         useDNAttribute="false"
1962         userDNAttribute="distinguishedName"
1963         userNameAttribute="uid"
1964         userContainer="o=spusers1lam"
1965         userObjectClass="person"
1966         userFilter="(ObjectClass=person) "
1967         scope="Subtree"
1968         otherRequiredUserAttributes="sn,givenname,cn"/>
1969     </providers>
1970 </membership>
1971 </system.web>
```

1972 To leverage RadiantOne Federated Identity for the SharePoint people picker, add the following line in  
1973 the <PeoplePickerWildcards> section of the web.config files for the SharePoint site and the Central Ad-  
1974 min (where VDSMembership is the name of the custom membership provider used):

```
1975 <add key="VDSMembership" value="*" />
1976 <PeoplePickerWildcards> <clear />
1977 <add key="AspNetSqlMembershipProvider" value="%" />
1978 <add key="VDSMembership" value="*" /> </PeoplePickerWildcards>
```

## 1979 2.8 Splunk

1980 Splunk is a Security Information and Event Management system that allows for the collection and  
1981 parsing of logs and data from multiple systems.

### 1982 2.8.1 How It's Used

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

## 2.8.2 Installation

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

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

- Windows
  - GUI: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonWindows>
  - Command line: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonWindowsviahecommandline>
- Linux: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonLinux>
- Solaris: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonSolaris>
- Mac OS X: <http://docs.splunk.com/Documentation/Splunk/6.5.2/Installation/InstallonMacOS>

## 2.8.3 Queries

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

## 2.8.4 Query: Detect User Provisioning Accounts Events

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

```
(index=main sourcetype="wineventlog:security" EventCode=5136 OR EventCode=4720) OR
(index=sandbox sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest") OR
(index=main sourcetype="openldap-outlog")|rex "givenName:(?P<FirstName>\w+)"|rex
"sn:(?P<LastName>\w+)"|rex mode=sed "s/;/ /g"|rex
"changetype:(?P<RLICHANGETYPE>\w+)"|rex "employeeNumber:(?P<EmployeeNumber>\w+)"|rex
"changetype:modify (?P<CHANGE>.+)"|rex "conn=\d+\s\w+\.cn=(?P<LDAP_UID>\w+\S\w+)"|rex
"A user account was (?P<RLICHANGETYPE>\w+)"|rex "A directory service object was
(?P<RLICHANGETYPE>\w+)"|eval
RLICHANGETYPE=if (RLICHANGETYPE=="modified","update",RLICHANGETYPE)|eval
RLICHANGETYPE=if (RLICHANGETYPE=="created","insert",RLICHANGETYPE)|eval
RLICHANGETYPE=if (RLICHANGETYPE=="add","insert",RLICHANGETYPE)|fields _time host
checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
```



```

2026 RLICHANGEType employeeNumber givenName sn uid gidnumber RLIANGES LDAP_UID LDAP_MSG
2027 AD_UID AD_MSG |rex "\-create\(\):User: (?P<LDAP_UID>\w+\.w+)"|rex "\-create\(\):User:
2028 (?P<AD_UID>\w+s)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.w+s\w+s\w+s)"|rex "\-
2029 create\(\):User: (?P<AD_MSG>\w+s\w+s\w+s)" |rex
2030 "<RLICHANGETYPE>(P<RLICHANGETYPE>\w+)"|rex
2031 "<RLICHANGES>(P<RLICHANGES>.)</RLICHANGES>"|rex "employeeNumber:
2032 (?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
2033 (?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\S+)"|rex
2034 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## 1: (?P<L>\w+)"|rex "## o:
2035 (?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
2036 "mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\S+s*\S+)"|rex
2037 "\<givenName>(P<GivenName>\S+s*\S+)</givenName>"|rex
2038 "\<sn>(P<SurName>\S+s*\S+)</sn>" |rex
2039 "\<employeeNumber>(P<EmployeeNumber>\S+s*\S+)</employeeNumber>" |table _time
2040 host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
2041 RLICHANGEType RLIANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
2042 LDAPUserId |where (isnotnull(FirstName)) OR (isnotnull(RLIANGES) OR
2043 (isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG))) OR isnotnull(RLICHANGEType) |eval
2044 F_Name=coalesce(FirstName,GivenName) |eval L_Name=coalesce(LastName,SurName) |eval
2045 EmpNo=coalesce(EmployeeNo,EmployeeNumber) |eval
2046 LDAP_UID=coalesce(LDAP_UID,LDAPUserId) |eval AD_UID=coalesce(AD_UserId,AD_UID) |table
2047 _time host checkStatus EmpNo F_Name L_Name RLICHANGEType RLIANGES checkAuthFields
2048 LDAP_UID AD_UID LDAP_MSG AD_MSG |eval RLIANGES=if(RLICHANGEType=="insert","New User
2049 Record",RLIANGES) |eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
2050 VDS"),lower(F_Name+"."+L_Name),LDAP_UID) |eval
2051 AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID) |eval
2052 RLIANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLIANGES) |eval
2053 RLIANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLIANGES) |eval
2054 RLIANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLIANGES) |eval
2055 RLIANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLIANGES) |eval
2056 UniqueKey=lower(LDAP_UID+"."+AD_UID) |eval host=if(host=="WIN-
2057 CHSUIS3NKVR","AlertEnterprise-WIN",host) |transaction UniqueKey, RLIANGES
2058 maxspan=120s |eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL") |eval
2059 host2=if(Like(host,"%WIN%"),"AlertE","NULL") |eval Authority=if((host1=="RadiantOne
2060 VDS" AND host2=="AlertE"), "Authorized", "Not Legal") |eval
2061 Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
2062 |table _time host Authority RLICHANGEType RLIANGES EmpNo F_Name L_Name LDAP_UID
2063 AD_UID ADCHANGEType |where isnotnull(EmpNo) |table _time host Authority RLICHANGEType
2064 RLIANGES EmpNo F_Name L_Name LDAP_UID AD_UID |where Authority != "Not Legal" |eval
2065 CHANGES=if(isnotnull(RLIANGES),RLIANGES,RLIANGES) |eval
2066 CHANGETYPE=if(isnotnull(RLICHANGEType),RLICHANGEType,RLICHANGEType) |table _time host
2067 Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID |where Not
2068 Like(CHANGES,"%lastLogonTimestamp")

```

## 2069 2.8.5 Query: Authorized and Unauthorized Provisioning Trend Line Chart

2070 The following search query generates a line chart showing the trends for both the authorized and  
 2071 unauthorized provisioning events:

```

2072 earliest="1/25/2017:00:00:00" latest="2/15/2017:00:00:00" index=sandbox
2073 sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest" |fields _time host
2074 checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId LDAPUserId
2075 RLICHANGEType employeeNumber givenName sn uid gidnumber RLIANGES LDAP_UID LDAP_MSG
2076 AD_UID AD_MSG |rex "\-create\(\):User: (?P<LDAP_UID>\w+\.w+)"|rex "\-create\(\):User:
2077 (?P<AD_UID>\w+s)"|rex "\-create\(\):User: (?P<LDAP_MSG>\w+\.w+s\w+s\w+s)"|rex "\-
2078 create\(\):User: (?P<AD_MSG>\w+s\w+s\w+s)" |rex
2079 "<RLICHANGETYPE>(P<RLICHANGETYPE>\w+)"|rex
2080 "<RLICHANGES>(P<RLICHANGES>.)</RLICHANGES>"|rex "employeeNumber:
2081 (?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
2082 (?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\S+)"|rex
2083 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## 1: (?P<L>\w+)"|rex "## o:
2084 (?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
2085 "mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\S+s*\S+)"|rex

```

```

2086 "\<givenName\>(P<GivenName>\S+\s*\S+)\</givenName\>"|rex
2087 "\<sn\>(P<SurName>\S+\s*\S+)\</sn\>"|rex
2088 "\<employeeNumber\>(P<EmployeeNumber>\S+\s*\S+)\</employeeNumber\>"|table _time
2089 host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
2090 RLICHANGEType RLIANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
2091 LDAPUserId|where (isnotnull(FirstName)) OR (isnotnull(RLIANGES) OR
2092 (isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG)))|eval
2093 F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
2094 EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
2095 LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID)|table
2096 _time host checkStatus EmpNo F_Name L_Name RLICHANGEType RLIANGES checkAuthFields
2097 LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLIANGES=if(RLICHANGEType=="insert","New User
2098 Record",RLIANGES)|eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
2099 VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
2100 AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
2101 RLIANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLIANGES)|eval
2102 RLIANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLIANGES)|eval
2103 RLIANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLIANGES)|eval
2104 RLIANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLIANGES)|eval
2105 UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
2106 CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLIANGES
2107 maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
2108 host2=if(Like(host,"%WIN%"),"AlertE","NULL")|eval Authority=if((host1=="RadiantOne
2109 VDS" AND host2=="AlertE"), "Authorized", "Not Legal")|eval
2110 Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
2111 |table _time host Authority RLICHANGEType RLIANGES EmpNo F_Name L_Name LDAP_UID
2112 AD_UID|where isnotnull(EmpNo)|table _time host Authority RLICHANGEType RLIANGES
2113 EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority != "Not Legal"|eval
2114 CHANGES=if(isnotnull(RLIANGES),RLIANGES,RLIANGES)|eval
2115 CHANGEType=if(isnotnull(RLICHANGEType),RLICHANGEType,RLICHANGEType)|table _time host
2116 Authority CHANGEType CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|timechart span=2d
2117 count BY Authority

```

## 2118 2.8.6 Query: Combined Provisioning Trend Line Chart

2119 The following search query generates a line chart that shows the total authorized and unauthorized  
 2120 provisioning events combined in a single trend line:

```

2121 index=sandbox sourcetype="alertstatictest" OR sourcetype="RadiantSourceTest"|fields
2122 _time host checkStatus checkAuthFields EmployeeNo FirstName LastName ADUserId
2123 LDAPUserId RLICHANGEType employeeNumber givenName sn uid gidnumber RLIANGES
2124 LDAP_UID LDAP_MSG AD_UID AD_MSG|rex "\-create\(\):User: (?P<LDAP_UID>\w+\.\w+)"|rex
2125 "\-create\(\):User: (?P<AD_UID>\w+\s+)"|rex "\-create\(\):User:
2126 (?P<LDAP_MSG>\w+\.\w+\s+\w+\s+\w+)"|rex "\-create\(\):User: (?P<AD_MSG>\w+\s+\w+\s+\w+)"
2127 |rex "<RLICHANGEType>(P<RLICHANGEType>\w+)"|rex
2128 "<RLIANGES>(P<RLIANGES>.+)\</RLIANGES\>"|rex "employeeNumber:
2129 (?P<EmployeeNumber>\w+)"|rex "sn: (?P<SurName>\w+)"|rex "givenName:
2130 (?P<GivenName>\w+)"|rex "gidNumber: (?P<GidNumber>\w+)"|rex "mail: (?P<mail>\S+)"|rex
2131 "departmentNumber: (?P<DeptNumber>\w+)"|rex "## 1: (?P<L>\w+)"|rex "## o:
2132 (?P<O>\w+)"|rex "## pager: (?P<Pager>\w+)"|rex "## initials: (?P<Initials>\w+)"|rex
2133 "mobile: (?P<Mobile>\w+)"|rex "modifiersName: (?P<ModifiersName>\S+\s*\S+)"|rex
2134 "\<givenName\>(P<GivenName>\S+\s*\S+)\</givenName\>"|rex
2135 "\<sn\>(P<SurName>\S+\s*\S+)\</sn\>"|rex
2136 "\<employeeNumber\>(P<EmployeeNumber>\S+\s*\S+)\</employeeNumber\>"|table _time
2137 host checkStatus EmployeeNo FirstName LastName EmployeeNumber GivenName SurName
2138 RLICHANGEType RLIANGES checkAuthFields LDAP_UID LDAP_MSG AD_UID AD_MSG ADUserId
2139 LDAPUserId|where (isnotnull(FirstName)) OR (isnotnull(RLIANGES) OR
2140 (isnotnull(LDAP_MSG)) OR (isnotnull(AD_MSG)))|eval
2141 F_Name=coalesce(FirstName,GivenName)|eval L_Name=coalesce(LastName,SurName)|eval
2142 EmpNo=coalesce(EmployeeNo,EmployeeNumber)|eval
2143 LDAP_UID=coalesce(LDAP_UID,LDAPUserId)|eval AD_UID=coalesce(AD_UserId,AD_UID)|table
2144 _time host checkStatus EmpNo F_Name L_Name RLICHANGEType RLIANGES checkAuthFields
2145 LDAP_UID AD_UID LDAP_MSG AD_MSG|eval RLIANGES=if(RLICHANGEType=="insert","New User

```

```

2146 Record",RLICHANGES)| eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
2147 VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
2148 AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
2149 RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2150 RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2151 RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2152 RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2153 UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
2154 CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
2155 maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
2156 host2=if(Like(host,"%WIN%"),"AlertE","NULL")|eval Authority=if((host1=="RadiantOne
2157 VDS" AND host2=="AlertE"),"Authorized", "Not Legal")|eval
2158 Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"), "Unauthorized", Authority)
2159 |table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
2160 AD_UID|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE RLICHANGES
2161 EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority != "Not Legal"|eval
2162 CHANGES=if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
2163 CHANGETYPE=if(isnotnull(RLICHANGETYPE),RLICHANGETYPE)|table _time host
2164 Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID |eval
2165 Event=if(isnotnull(Authority),"Provisioning", "Null")|timechart span=2d count BY Event

```

## 2166 2.8.7 Query: Detect modifications to High Value or Privileged Accounts

2167 The following search query detects any modification to high-value accounts or privileged accounts, such  
 2168 as managers and system administrators. It detects modifications that violate corporate policy as well as  
 2169 those that are performed in accordance to policy.

```

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

```

```

2205 Record",RLICHANGES)| eval LDAP_UID=if((isnull(LDAP_UID) AND host=="RadiantOne
2206 VDS"),lower(F_Name+"."+L_Name),LDAP_UID)|eval
2207 AD_UID=if(isnull(AD_UID),lower(substr(F_Name,1,1) + substr(L_Name,1)),AD_UID)|eval
2208 RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2209 RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2210 RLICHANGES=if(Like(LDAP_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2211 RLICHANGES=if(Like(AD_MSG,"%created%"),"New User Record",RLICHANGES)|eval
2212 UniqueKey=lower(LDAP_UID+"."+AD_UID)|eval host=if(host=="WIN-
2213 CHSUIS3NKVR","AlertEnterprise-WIN",host)|transaction UniqueKey, RLICHANGES
2214 maxspan=120s|eval host1=if(Like(host,"%RadiantOne VDS%"),"RadiantOne VDS","NULL")|eval
2215 host2=if(Like(host,"%WIN%"),"AlertE","NULL")|eval Authority=if((host1=="RadiantOne
2216 VDS" AND host2=="AlertE"),"Authorized","Not Legal")|eval
2217 Authority=if((host1=="RadiantOne VDS" AND host2=="NULL"),"Unauthorized", Authority)
2218 |table _time host Authority RLICHANGETYPE RLICHANGES EmpNo F_Name L_Name LDAP_UID
2219 AD_UID ADCHANGETYPE|where isnotnull(EmpNo)|table _time host Authority RLICHANGETYPE
2220 RLICHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Authority != "Not Legal"|eval
2221 CHANGES=if(isnotnull(RLICHANGES),RLICHANGES,RLICHANGES)|eval
2222 CHANGETYPE=if(isnotnull(RLICHANGETYPE),RLICHANGETYPE,RLICHANGETYPE)|table _time host
2223 Authority CHANGETYPE CHANGES EmpNo F_Name L_Name LDAP_UID AD_UID|where Not
2224 Like(CHANGES, "%lastLogonTimestamp")|table _time host Authority CHANGETYPE CHANGES
2225 EmpNo F_Name L_Name LDAP_UID AD_UID|where isnotnull(CHANGETYPE) AND ((Like(CHANGES,
2226 "%MNGR%")) OR (Like(CHANGES, "%Manager%") OR Like(CHANGES, "%Administrator%")))

```

## 2227 2.8.8 Query: Virtual Directory Server Offline Detection

2228 The following search query detects when the virtual directory server goes offline. The virtual directory  
 2229 server is configured to send online status messages to Splunk at regular intervals. This query searches  
 2230 for those messages and declares the virtual directory server offline if the last online message received  
 2231 has exceeded the expected interval.

```

2232 earliest=-24h sourcetype="radiant-status"|table _time CurrentTime Hostname Status|sort
2233 1 -_time|eval SearchTime_Epoch=now()|eval CTime_Epoch=strptime(CurrentTime,"%a %b %d
2234 %H:%M:%S %Z %Y")|eval TimeDiff=(SearchTime_Epoch - CTime_Epoch)|eval Status=if(TimeDiff
2235 > 900, "Offline", Status)|where Status=="offline"|table CurrentTime Hostname Status

```

## 2236 2.8.9 Query: Critical Servers Offline

2237 The following search query detects when a directory server goes offline. The query uses the results of  
 2238 multiple data sources to determine when a server is offline and when it is online.

```

2239 earliest=-12h (index=sandbox sourcetype="radiantsourcetest" ERROR) OR (index=main
2240 sourcetype=openldap-status1) OR (index=main sourcetype=AD-Status) OR
2241 (sourcetype="Vanguard-Status") OR (sourcetype="Radiant-Status") |rex "Exception taking
2242 snapshot. Entries in snapshot: 0 Error :com.rli.slapped.server.LDAPException:
2243 (?P<IPAddress>\d+\.\d+\.\d+\.\d+)"|rex "ERROR (?P<ConnectionStatus>\w+\s\w+)"|table
2244 _time CurrentTime PrevTime Hostname Status IPAddress ConnectionStatus|eval
2245 CTime=strptime(CurrentTime,"%a %b %d %H:%M:%S %Z %Y")|eval PTime=strptime(PrevTime,"%a
2246 %b %d %H:%M:%S %Z %Y")|eval TimeDiff=(CTime-PTime)|eval
2247 Hostname=if(IPAddress=="192.168.19.11", "openldap.acmefinancial.com", Hostname)|eval
2248 Hostname=if(IPAddress=="192.168.19.10", "ActiveDirectory.acmefinancial.com",
2249 Hostname)|eval Hostname=if(Hostname=="RadiantOne VDS", "RadiantOne
2250 VDS.acmefinancial.com", Hostname)|eval Hostname=if(Hostname=="ActiveDirectory",
2251 "ActiveDirectory.acmefinancial.com", Hostname)|eval
2252 Status=if(ConnectionStatus=="Connection error", "offline", Status)|where
2253 isnotnull(Hostname)|transaction Hostname Status|table _time Hostname Status

```

## 2254 2.8.10 SSL Forwarding

2255 We took advantage Splunk's built in SSL forwarding capability and configured SSL encryption between  
 2256 forwarders and the indexer. Instructions to enable SSL forwarding can be found at

2257 [http://docs.splunk.com/Documentation/Splunk/6.5.3/Security/ConfigureSplunkforwardingtousesignedc](http://docs.splunk.com/Documentation/Splunk/6.5.3/Security/ConfigureSplunkforwardingtousesignedcertificates)  
 2258 [ertificates.](http://docs.splunk.com/Documentation/Splunk/6.5.3/Security/ConfigureSplunkforwardingtousesignedcertificates)

## 2259 2.9 TDI ConsoleWorks

2260 ConsoleWorks is a product that provides a portal for remote access to devices, a logging facility with  
 2261 advanced hashing and pattern matching features, and role-based access control for administrators.

### 2262 2.9.1 How It's Used

2263 ConsoleWorks provides a portal through which privileged users access directory servers and core  
 2264 systems in the lab infrastructure. There are two primary types of access connectors that are configured.  
 2265 The first is a console connector that is either an SSH or Telnet connection to an internal LAN system. The  
 2266 other is a graphical user interface (GUI) connector that can be either through Remote Desktop Protocol  
 2267 (RDP) or Virtual Network Computing (VNC). In this build, SSH was used for the console connections,  
 2268 whereas RDP was used for the GUI connections.

2269 The ConsoleWorks Server sits on a separate subnet that is connected to the Internet via a virtual private  
 2270 network. It is configured to allow connections initiated from the VPN, but it drops connections initiated  
 2271 from the LAN.

2272 Additionally, ConsoleWorks maintains logs of what systems were accessed, the time of access, and by  
 2273 whom. These logs are formatted and prepared for consumption by the Splunk indexer.

### 2274 2.9.2 Virtual Machine Configuration

2275 ConsoleWorks virtual machine is configured as follows:

- 2276     ▪ CentOS 7.2.1511
- 2277     ▪ 1CPU cor
- 2278     ▪ 8GB of RAM
- 2279     ▪ 2 NICs
- 2280     ▪ 100GB of storage.

#### 2281 **Network Configuration (LAN)**

2282 IPv4 Manual  
 2283 IPv6 Enabled  
 2284 IP Address: 192.168.17.11  
 2285 Netmask: 255.255.255.0  
 2286 Gateway: 192.168.17.1  
 2287 DNS Name Servers 192.168.19.10  
 2288 DNS-Search Domains: acmefinancial.com

#### 2289 **Network Configuration (WAN)**

2290 IPv4 Manual  
 2291 IPv6 Enabled  
 2292 IP Address: 10.33.50.164  
 2293 Netmask: 255.255.240.0

### 2294 2.9.3 Firewall Configuration



2295 Enter the following commands in sequence to allow traffic to ports 5176 and 22 ports only. The  
 2296 ConsoleWorks web service listens on port 5176.

- 2297 1. **firewall-cmd – zone=public – add-port=5176/tcp**
- 2298 2. **firewall-cmd – zone=public – add-port=22/tcp**

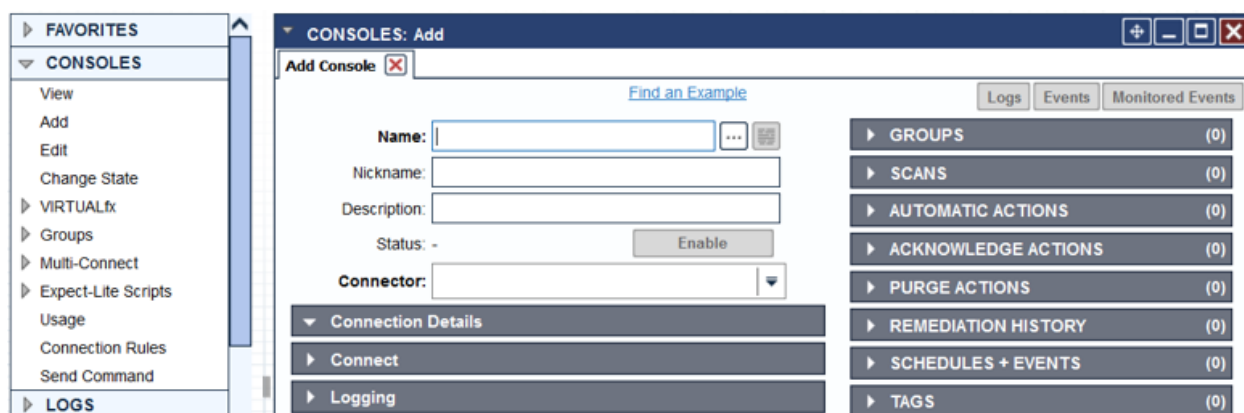
## 2299 2.9.4 Installation

2300 Installation for Windows, Linux, and Solaris systems can be found at  
 2301 <http://support.tditechnologies.com/tags/installation-guides>

## 2302 2.9.5 Console Connection Configuration

2303 To create a console connection:

- 2304 1. Click on **Consoles>Add**.
- 2305 2. Type in the name of the Console (for example, **OpenLDAPServer**).
- 2306 3. Choose the **Connector** type (for example, **SSH on Demand**).
- 2307 4. Click **Connection Details**. Check the **Exclusive Connect** checkbox.
- 2308 5. Type in the **Host IP**, **Port**, **Username**, and **Password** fields.
- 2309 6. Click **Save**.



## 2311 2.9.6 Graphical Gateway Configuration

2312 A Graphical Gateway is required to make an RDP or VNC connection to a server.

2313 To configure a Graphical Gateway, you need to obtain and install the graphical gateway package from  
 2314 TDi Technologies Inc. The following steps describe installing and starting the service once the package is  
 2315 obtained.

```
2316 rpm -ivh /tmp/consoleworks/ConsoleWorks_gui_gateway-version>.rpm
2317 /opt/gui_gateway/install_local.sh
2318 /opt/ConsoleWorks/bin/cw_start <invocation name> (created during installation)
2319 service gui_gatewayd start
```

2320 Install the Graphical gateway:

- 2321 1. On the landing page on your ConsoleWorks server, click **GRAPHICAL>Gateways>Add**.
- 2322 2. Give it a name, then set **Host** as Localhost and **Port** as 5172.
- 2323 3. Check **Enabled** checkbox and click **Save**.
- 2324 4. Verify it works by clicking **Test** in the top-left corner.

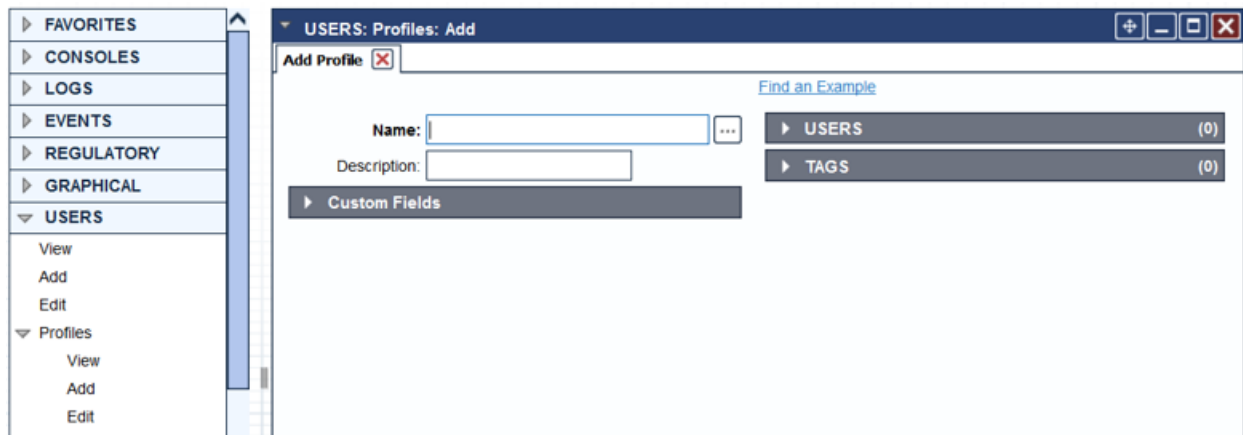
## 2.9.7 Graphical Connection Configuration

Configure the Graphical gateway:

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

## 2.9.8 Profile Creation

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



### 2.9.9 Access Controls

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

Create new access control rules:

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



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       |  |

Delete

Add

Examples

Copy

Rename

Edit

- 2350
- 2351
- 2352
- 2353
- 2354
- 2355
- 2356
- 2357
- To create a profile:
1.

In the **Allow or Deny** field, Select **ALLOW**.
2.

In the component **Type**, select **Console**.
3.

In the **Profile Selection** area, select the profile of choice from the **Simple** tab and click the double arrows. Make sure it appears in the **Profiles** section.
4.

In the **Resource Selection** section, select the Console you want users associated with this profile to connect to. Select the **OpenLDAP** console.

SECURITY: Access Control: Edit \*

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

History

Name: COPY\_CONSOLE\_CONTROL ...

Description: Sample Console CONTROL access

☒ Enabled

Order: 50

Allow or Deny: ALLOW

☐ Audit Rule Usage

Component Type: Console

Profile Selection

Simple Basic Advanced Profiles

DEFAULT TESTPI

RADIANTLOGICPROFILE RADIAN

RADIANTLOGICPROFILE TESTPROFILE

Resource Selection

Simple Basic Advanced Consoles

Selection:

- Property Console Equals OpenLDAP <join>

+ OPENLDAP

Set As Default Save As... Delete Cancel Save

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**.

SECURITY: Access Control: View

View Access Control Rules

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

Delete

Add

Examples

Copy

Rename

Edit

- 2362
- 2363
- 2364
- 2365
- 2366
- 2367
- 2368
- 2369
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.

**SECURITY: Access Control: Edit**

View Access Control Rules ☐ Edit Access Control Rule ☒

**History**

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

**Description:** Default ALLOW Graphical Connection

☒ Enabled

**Order:** 99940

**Allow or Deny:** ALLOW

☐ Audit Rule Usage

**Component Type:** Graphical Connection

**Profile Selection**

Simple Basic Advanced Profiles

Is one of these Profiles

☐ All Profiles

| Profile             | Select                   |
|---------------------|--------------------------|
| CONSOLE_MANAGER     | <input type="checkbox"/> |
| DEFAULT             | <input type="checkbox"/> |
| RADIANTLOGICPROFILE | <input type="checkbox"/> |

**Resource Selection**

Set As Default Save As... Delete Cancel Save

- 2370
- 2371 1. Next, you will need to **Select** the Graphical Connection of choice such as RADIANTONE VDS.
- 2372 2. Click the double arrow and ensure that it appears on the right.

**SECURITY: Access Control: Edit**

View Access Control Rules ☒ Edit Access Control Rule ☒

**History**

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

**Description:** Default ALLOW Graphical Connection

☒ Enabled

**Order:** 99940

**Allow or Deny:** ALLOW

☐ Audit Rule Usage

**Component Type:** Graphical Connection

**Profile Selection**

**Resource Selection**

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

Is one of these Graphical Connections

☐ All Graphical Connections

**Graphical Connection** **Select**

ADTEST /

RADIANTONEVDS |

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

2373

2374 To add users and link to a profile:

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

2379 5. Select the profile of choice.

**USERS: Add**

Add User ☒

[Find an Example](#)

**Name:**

**Description:**

**Login Expiration:**

**User Created:**

**Last Login:**

☐ Use External Authentication

**Password**

**Password:**

**Retype Password:**

☒ Require Password Change On Next Login

**Password Rules**

**Contact Info**

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

2380

## 2381 2.9.10 pUser Auditing

2382 An audit trail of ConsoleWorks user activity is captured in a file and forwarded to Splunk for further  
 2383 analysis. The the information includes username, logon timestamp, and the target server to which the  
 2384 user is connecting. The connection reporting script below parses the ConsoleWorks logs and writes the  
 2385 output to a file. The bash connectionreporting script removes duplicate lines. The  
 2386 bashconenctionreporting script is scheduled using cron to run every minute using the following  
 2387 /etc/crontab configuration.

## 2388 2.9.11 Cron Configuration: /etc/crontab

```
2389 SHELL=/bin/bash
2390 PATH=/sbin:/bin:/usr/sbin:/usr/bin
2391 MAILTO=root
2392 # For details see man 4 crontabs
2393 # Example of job definition:
2394 # .----- minute (0 - 59)
2395 # | .----- hour (0 - 23)
2396 # | | .----- day of month (1 - 31)
2397 # | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
2398 # | | | | .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
2399 # | | | | |
2400 # * * * * * user-name command to be executed
2401 * * * * * root /etc/cron.daily/bashconnectionreporting
```

## 2402 2.9.12 Scripts: connectionreporting

```
2403 #!/usr/bin/python3.5
2404 #Script identifies ConsoleWorks users, connection times and their targets
2405 #import the OS module
2406 import os
2407 #Store the ConsoleWorks log directory in the "directory" variable
2408 directory = "/opt/ConsoleWorks/FSARM/log"
2409 #Change directory to the Log dir
2410 os.chdir(directory)
2411 #Iterate through files in log dir and look for strings shown in the
2412 #IF statements. Matching lines are written to file
2413 for file in os.listdir(directory):
2414     with open(file, 'r') as file_object:
2415         for line in file_object:
2416             if "CONWRKS Audit:: User:" in line:
2417                 with open('/var/log/connections.out','a') as outfile_object:
2418                     outfile_object.write(line)
2419             if "connecting" in line:
```

```

2420         with open('/var/log/connections.out','a') as outfile_object:
2421             outfile_object.write(line)
2422     if "disconnecting" in line:
2423         with open('/var/log/connections.out','a') as outfile_object:
2424             outfile_object.write(line)

```

### 2425 2.9.13 Scripts: bashconnectionreporting

```

2426 #!/bin/bash
2427 #Calls python script that reads ConsoleWorks log files and outputs to
2428 #/var/log/connections.out
2429 /etc/cron.daily/connectionreporting
2430 #This line removes duplicate lines from the connections.out file and outputs them
2431 # to connections.log
2432 awk '!seen[$0]++' /var/log/connections.out > /var/log/connections.log

```

## 2433 2.10 Network Firewall Configuration

2434 pfSense virtual devices were used as firewall routers for each subnet and were configured to restrict  
2435 traffic as appropriate. The subnets listed below have critical services and resources that need to be  
2436 accessed from devices external to the LAN. We have made the exact configuration used in each pfSense  
2437 firewall available in XML format. This can be imported directly into another pfSense device. It is  
2438 important to note that an IPSEC VPN connection was made to the offsite RACF LDAP directory server.  
2439 The IPSEC VPN configuration was set up in the firewall for the backbone subnet.

### 2440 2.10.1 Firewall Configuration for Backbone Subnet

```

2441 <?xml version="1.0"?>
2442 <pfsense>
2443     <version>15.4</version>
2444     <lastchange/>
2445     <theme>pfsense_ng</theme>
2446     <system>
2447         <optimization>normal</optimization>
2448         <hostname>pfsenseVLAN13</hostname>
2449         <domain>acmefinancial.com</domain>
2450         <group>
2451             <name>all</name>
2452             <description><![CDATA[All Users]]></description>
2453             <scope>system</scope>
2454             <gid>1998</gid>
2455             <member>0</member>
2456         </group>
2457     </system>
2458     <name>admins</name>

```

```

2459         <description><![CDATA[System Administrators]]></description>
2460         <scope>system</scope>
2461         <gid>1999</gid>
2462         <member>0</member>
2463         <priv>page-all</priv>
2464     </group>
2465     <user>
2466         <name>admin</name>
2467         <descr><![CDATA[System Administrator]]></descr>
2468         <scope>system</scope>
2469         <groupname>admins</groupname>
2470         <password>$1$dSJmFph$GvZ7.1UbuWu.Yb8etC0re.</password>
2471         <uid>0</uid>
2472         <priv>user-shell-access</priv>
2473     </user>
2474     <nextuid>2000</nextuid>
2475     <nextgid>2000</nextgid>
2476     <timezone>America/New_York</timezone>
2477     <time-update-interval/>
2478     <timeservers>10.97.74.8</timeservers>
2479     <webgui>
2480         <protocol>http</protocol>
2481         <loginautocomplete/>
2482         <ssl-certref>5720a0502b277</ssl-certref>
2483         <dashboardcolumns>2</dashboardcolumns>
2484         <webguicss>pfsense.css</webguicss>
2485     </webgui>
2486     <disablesegmentationoffloading/>
2487     <disablelargereceiveoffloading/>
2488     <ipv6allow/>
2489     <powerd_ac_mode>hadp</powerd_ac_mode>
2490     <powerd_battery_mode>hadp</powerd_battery_mode>
2491     <powerd_normal_mode>hadp</powerd_normal_mode>
2492     <bogons>
2493         <interval>monthly</interval>
2494     </bogons>
2495     <language>en_US</language>
2496     <dns1gw>GW_WAN</dns1gw>
2497     <dns2gw>GW_WAN</dns2gw>
2498     <dns3gw>none</dns3gw>

```



```

2499         <dns4gw>none</dns4gw>
2500         <maximumstates/>
2501         <aliasesresolveinterval/>
2502         <maximumtableentries/>
2503         <maximumfrags/>
2504         <enablenatreflectionpurenat>yes</enablenatreflectionpurenat>
2505         <enablebinatreflection>yes</enablebinatreflection>
2506         <enablenatreflectionhelper>yes</enablenatreflectionhelper>
2507         <reflectiontimeout/>
2508         <dnsserver>10.97.74.8</dnsserver>
2509         <dnsserver>10.63.255.2</dnsserver>
2510     </system>
2511     <interfaces>
2512         <wan>
2513             <if>em0</if>
2514             <descr><![CDATA[WAN]]></descr>
2515             <enable/>
2516             <spoofmac/>
2517             <ipaddr>10.33.50.34</ipaddr>
2518             <subnet>28</subnet>
2519             <gateway>GW_WAN</gateway>
2520             <ipaddrv6/>
2521             <subnetv6/>
2522             <gatewayv6/>
2523         </wan>
2524         <lan>
2525             <enable/>
2526             <if>em1</if>
2527             <ipaddr>192.168.13.1</ipaddr>
2528             <subnet>24</subnet>
2529             <ipaddrv6/>
2530             <subnetv6/>
2531             <media/>
2532             <mediaopt/>
2533             <track6-interface>wan</track6-interface>
2534             <track6-prefix-id>0</track6-prefix-id>
2535             <gateway/>
2536             <gatewayv6/>
2537         </lan>
2538     </interfaces>

```

```

2539     <staticroutes>
2540         <route>
2541             <network>192.168.14.0/24</network>
2542             <gateway>VLAN2014</gateway>
2543             <descr/>
2544         </route>
2545         <route>
2546             <network>192.168.19.0/24</network>
2547             <gateway>VLAN2019</gateway>
2548             <descr/>
2549         </route>
2550         <route>
2551             <network>192.168.18.0/24</network>
2552             <gateway>VLAN2018</gateway>
2553             <descr/>
2554         </route>
2555         <route>
2556             <network>192.168.15.0/24</network>
2557             <gateway>VLAN2015</gateway>
2558             <descr/>
2559         </route>
2560         <route>
2561             <network>192.168.16.0/24</network>
2562             <gateway>VLAN2016</gateway>
2563             <descr/>
2564         </route>
2565         <route>
2566             <network>192.168.17.0/24</network>
2567             <gateway>VLAN2017</gateway>
2568             <descr/>
2569         </route>
2570         <route>
2571             <network>192.168.20.0/24</network>
2572             <gateway>VLAN2020</gateway>
2573             <descr/>
2574         </route>
2575         <route>
2576             <network>10.33.50.160/28</network>
2577             <gateway>VLAN2066</gateway>
2578             <descr><![CDATA[Route to Vendor Net]]></descr>

```

```

2579         </route>
2580     </staticroutes>
2581     <dhcpd>
2582         <lan>
2583             <enable/>
2584             <range>
2585                 <from>192.168.13.100</from>
2586                 <to>192.168.13.150</to>
2587             </range>
2588             <failover_peerip/>
2589             <dhcpleaseinlocaltime/>
2590             <defaultleasetime/>
2591             <maxleasetime/>
2592             <netmask/>
2593             <dnsserver>192.168.19.10</dnsserver>
2594             <gateway/>
2595             <domain>acmefinancial.com</domain>
2596             <domainsearchlist>acmefinancial.com</domainsearchlist>
2597             <ddnsdomain/>
2598             <ddnsdomainprimary/>
2599             <ddnsdomainkeyname/>
2600             <ddnsdomainkey/>
2601             <mac_allow/>
2602             <mac_deny/>
2603             <tftp/>
2604             <ldap/>
2605             <nextserver/>
2606             <filename/>
2607             <filename32/>
2608             <filename64/>
2609             <rootpath/>
2610             <numeroptions/>
2611         </lan>
2612         <opt1>
2613             <enable/>
2614             <range>
2615                 <from>192.168.14.100</from>
2616                 <to>192.168.14.150</to>
2617             </range>
2618             <dhcpleaseinlocaltime/>

```

## DRAFT

```

2619         </opt1>
2620         <opt2>
2621             <enable/>
2622             <range>
2623                 <from>192.168.15.100</from>
2624                 <to>192.168.15.150</to>
2625             </range>
2626             <dhcpleaseinlocaltime/>
2627         </opt2>
2628         <opt3>
2629             <enable/>
2630             <range>
2631                 <from>192.168.16.100</from>
2632                 <to>192.168.16.150</to>
2633             </range>
2634             <dhcpleaseinlocaltime/>
2635         </opt3>
2636     </dhcpd>
2637     <snmpd>
2638         <syslocation/>
2639         <syscontact/>
2640         <rocommunity>public</rocommunity>
2641     </snmpd>
2642     <diag>
2643         <ipv6nat>
2644             <ipaddr/>
2645         </ipv6nat>
2646     </diag>
2647     <bridge/>
2648     <syslog/>
2649     <nat>
2650         <outbound>
2651             <mode>automatic</mode>
2652         </outbound>
2653         <onetoone>
2654             <external>10.33.50.44</external>
2655             <descr><![CDATA[mapping to 2020 pfsense firewall ]]></descr>
2656             <interface>wan</interface>
2657             <source>
2658                 <address>192.168.13.20</address>

```

```

2659         </source>
2660         <destination>
2661             <any/>
2662         </destination>
2663     </onetoone>
2664     <onetoone>
2665         <external>10.33.50.42</external>
2666         <descr><![CDATA[Mapping to Pfsense firewall]]></descr>
2667         <interface>wan</interface>
2668         <source>
2669             <address>192.168.13.17</address>
2670         </source>
2671         <destination>
2672             <any/>
2673         </destination>
2674     </onetoone>
2675     <onetoone>
2676         <external>10.33.50.35</external>
2677         <descr><![CDATA[Mapping to Splunk]]></descr>
2678         <interface>wan</interface>
2679         <source>
2680             <address>192.168.17.11</address>
2681         </source>
2682         <destination>
2683             <any/>
2684         </destination>
2685     </onetoone>
2686     <onetoone>
2687         <external>10.33.50.41</external>
2688         <descr><![CDATA[Mapping to Pfsense firewall]]></descr>
2689         <interface>wan</interface>
2690         <source>
2691             <address>192.168.19.11</address>
2692         </source>
2693         <destination>
2694             <any/>
2695         </destination>
2696     </onetoone>
2697     <onetoone>
2698         <external>10.33.50.36</external>

```

```

2699         <descr><![CDATA[Mapping to Hytrust ESXi Server]]></descr>
2700         <interface>wan</interface>
2701         <source>
2702             <address>192.168.20.12</address>
2703         </source>
2704         <destination>
2705             <any/>
2706         </destination>
2707     </onetoone>
2708     <onetoone>
2709         <external>10.33.50.37</external>
2710         <descr><![CDATA[NAT Mapping to RadiantOne VDS]]></descr>
2711         <interface>wan</interface>
2712         <source>
2713             <address>192.168.14.11</address>
2714         </source>
2715         <destination>
2716             <any/>
2717         </destination>
2718     </onetoone>
2719     <onetoone>
2720         <external>10.33.50.38</external>
2721         <descr><![CDATA[NAT Mapping to Hytrust CloudControl VM]]></descr>
2722         <interface>wan</interface>
2723         <source>
2724             <address>192.168.20.11</address>
2725         </source>
2726         <destination>
2727             <any/>
2728         </destination>
2729     </onetoone>
2730     <onetoone>
2731         <external>10.33.50.40</external>
2732         <descr><![CDATA[Mapping to ActiveDirectory]]></descr>
2733         <interface>wan</interface>
2734         <source>
2735             <address>192.168.19.10</address>
2736         </source>
2737         <destination>
2738             <any/>

```

```

2739             </destination>
2740         </onetoone>
2741         <onetoone>
2742             <external>10.33.50.43</external>
2743             <descr><![CDATA[VIP for ConsoleWorks -- Mapping to Internal
2744 Address]]></descr>
2745             <interface>wan</interface>
2746             <source>
2747                 <address>192.168.17.11</address>
2748             </source>
2749             <destination>
2750                 <any/>
2751             </destination>
2752         </onetoone>
2753         <onetoone>
2754             <external>10.33.50.45</external>
2755             <descr><![CDATA[VIP for CentOSToAD-- Mapping to Internal
2756 Address]]></descr>
2757             <interface>wan</interface>
2758             <source>
2759                 <address>192.168.19.30</address>
2760             </source>
2761             <destination>
2762                 <any/>
2763             </destination>
2764         </onetoone>
2765         <onetoone>
2766             <external>10.33.50.46</external>
2767             <descr><![CDATA[AlertEnterprise Enterprise Guardian]]></descr>
2768             <interface>wan</interface>
2769             <source>
2770                 <address>192.168.17.114</address>
2771             </source>
2772             <destination>
2773                 <any/>
2774             </destination>
2775         </onetoone>
2776         <rule>
2777             <source>
2778                 <any/>

```

```

2779         </source>
2780         <destination>
2781             <network>wanip</network>
2782             <port>1322</port>
2783         </destination>
2784         <protocol>tcp</protocol>
2785         <target>192.168.13.130</target>
2786         <local-port>80</local-port>
2787         <interface>wan</interface>
2788         <descr><![CDATA[Mapping to pfsense 192.168.13.130]]></descr>
2789         <associated-rule-id>nat_581795efbc2944.51341500</associated-rule-
2790 id>
2791         <created>
2792             <time>1477940719</time>
2793             <username>admin@192.168.13.139</username>
2794         </created>
2795         <updated>
2796             <time>1477940861</time>
2797             <username>admin@192.168.13.139</username>
2798         </updated>
2799     </rule>
2800     <rule>
2801         <source>
2802             <any/>
2803         </source>
2804         <destination>
2805             <address>10.33.50.41</address>
2806             <port>80</port>
2807         </destination>
2808         <protocol>tcp/udp</protocol>
2809         <target>192.168.19.11</target>
2810         <local-port>80</local-port>
2811         <interface>wan</interface>
2812         <descr><![CDATA[Port forward to openldap; Add /phpldapadmin to
2813 address]]></descr>
2814         <associated-rule-id>nat_57bf0c96d083f4.07194849</associated-rule-
2815 id>
2816         <created>
2817             <time>1472138390</time>
2818             <username>admin@10.97.67.137</username>
2819         </created>

```



```

2820         <updated>
2821             <time>1473431620</time>
2822             <username>admin@10.97.67.134</username>
2823         </updated>
2824     </rule>
2825     <rule>
2826         <source>
2827             <any/>
2828         </source>
2829         <destination>
2830             <address>10.33.50.41</address>
2831             <port>22</port>
2832         </destination>
2833         <protocol>tcp/udp</protocol>
2834         <target>192.168.19.11</target>
2835         <local-port>22</local-port>
2836         <interface>wan</interface>
2837         <descr><![CDATA[Port forward to openldap; ]]></descr>
2838         <associated-rule-id>nat_57f555406f2de3.01889708</associated-rule-
2839 id>
2840         <created>
2841             <time>1475695936</time>
2842             <username>admin@10.97.67.145</username>
2843         </created>
2844         <updated>
2845             <time>1475695966</time>
2846             <username>admin@10.97.67.145</username>
2847         </updated>
2848     </rule>
2849     <rule>
2850         <source>
2851             <any/>
2852         </source>
2853         <destination>
2854             <address>10.33.50.35</address>
2855             <port>8000</port>
2856         </destination>
2857         <protocol>tcp/udp</protocol>
2858         <target>192.168.17.10</target>
2859         <local-port>8000</local-port>

```

```

2860         <interface>wan</interface>
2861         <descr><![CDATA[Splunk port 8000 Web Interface]]></descr>
2862         <associated-rule-id>nat_57d825ba865df6.65796295</associated-rule-
2863 id>
2864         <created>
2865             <time>1473783226</time>
2866             <username>admin@10.97.67.152</username>
2867         </created>
2868         <updated>
2869             <time>1473785552</time>
2870             <username>admin@10.97.67.152</username>
2871         </updated>
2872     </rule>
2873     <rule>
2874         <source>
2875             <any/>
2876         </source>
2877         <destination>
2878             <address>10.33.50.35</address>
2879             <port>22</port>
2880         </destination>
2881         <protocol>tcp/udp</protocol>
2882         <target>192.168.17.10</target>
2883         <local-port>22</local-port>
2884         <interface>wan</interface>
2885         <descr><![CDATA[Splunk SSH ]]></descr>
2886         <associated-rule-id>nat_582ef78ed63d23.63868026</associated-rule-
2887 id>
2888         <updated>
2889             <time>1479473038</time>
2890             <username>admin@10.97.67.135</username>
2891         </updated>
2892         <created>
2893             <time>1479473038</time>
2894             <username>admin@10.97.67.135</username>
2895         </created>
2896     </rule>
2897     <rule>
2898         <source>
2899             <any/>

```

```

2900         </source>
2901         <destination>
2902             <address>10.33.50.42</address>
2903             <port>1314</port>
2904         </destination>
2905         <protocol>tcp/udp</protocol>
2906         <target>192.168.13.14</target>
2907         <local-port>80</local-port>
2908         <interface>wan</interface>
2909         <descr><![CDATA[Port Forward to 192.168.13.14 Pf]]></descr>
2910         <associated-rule-id>nat_57c01545c247f0.43308393</associated-rule-
2911 id>
2912         <updated>
2913             <time>1472206149</time>
2914             <username>admin@10.97.67.135</username>
2915         </updated>
2916         <created>
2917             <time>1472206149</time>
2918             <username>admin@10.97.67.135</username>
2919         </created>
2920     </rule>
2921     <rule>
2922         <source>
2923             <any/>
2924         </source>
2925         <destination>
2926             <address>10.33.50.42</address>
2927             <port>1315</port>
2928         </destination>
2929         <protocol>tcp/udp</protocol>
2930         <target>192.168.13.15</target>
2931         <local-port>80</local-port>
2932         <interface>wan</interface>
2933         <descr><![CDATA[Port Forward to 192.168.13.15 Pf]]></descr>
2934         <associated-rule-id>nat_57c0163d6e2de9.62906352</associated-rule-
2935 id>
2936         <updated>
2937             <time>1472206397</time>
2938             <username>admin@10.97.67.135</username>
2939         </updated>

```

```

2940         <created>
2941             <time>1472206397</time>
2942             <username>admin@10.97.67.135</username>
2943         </created>
2944     </rule>
2945     <rule>
2946         <source>
2947             <any/>
2948         </source>
2949         <destination>
2950             <address>10.33.50.42</address>
2951             <port>1316</port>
2952         </destination>
2953         <protocol>tcp/udp</protocol>
2954         <target>192.168.13.16</target>
2955         <local-port>80</local-port>
2956         <interface>wan</interface>
2957         <descr><![CDATA[Port Forward to 192.168.13.16 Pf]]></descr>
2958         <associated-rule-id>nat_57c01682da98c4.72334719</associated-rule-
2959 id>
2960         <updated>
2961             <time>1472206466</time>
2962             <username>admin@10.97.67.135</username>
2963         </updated>
2964         <created>
2965             <time>1472206466</time>
2966             <username>admin@10.97.67.135</username>
2967         </created>
2968     </rule>
2969     <rule>
2970         <source>
2971             <any/>
2972         </source>
2973         <destination>
2974             <address>10.33.50.42</address>
2975             <port>1317</port>
2976         </destination>
2977         <protocol>tcp/udp</protocol>
2978         <target>192.168.13.17</target>
2979         <local-port>80</local-port>

```

```

2980         <interface>wan</interface>
2981         <descr><![CDATA[Port Forward to 192.168.13.17 Pf]]></descr>
2982         <associated-rule-id>nat_57c01787b4e891.75909166</associated-rule-
2983 id>
2984         <updated>
2985             <time>1472206727</time>
2986             <username>admin@10.97.67.135</username>
2987         </updated>
2988         <created>
2989             <time>1472206727</time>
2990             <username>admin@10.97.67.135</username>
2991         </created>
2992     </rule>
2993     <rule>
2994         <source>
2995             <any/>
2996         </source>
2997         <destination>
2998             <address>10.33.50.42</address>
2999             <port>1318</port>
3000         </destination>
3001         <protocol>tcp/udp</protocol>
3002         <target>192.168.13.18</target>
3003         <local-port>80</local-port>
3004         <interface>wan</interface>
3005         <descr><![CDATA[Port Forward to 192.168.13.18 Pf]]></descr>
3006         <associated-rule-id>nat_57c017be3dffaf.16882401</associated-rule-
3007 id>
3008         <updated>
3009             <time>1472206782</time>
3010             <username>admin@10.97.67.135</username>
3011         </updated>
3012         <created>
3013             <time>1472206782</time>
3014             <username>admin@10.97.67.135</username>
3015         </created>
3016     </rule>
3017     <rule>
3018         <source>
3019             <any/>

```

```

3020         </source>
3021         <destination>
3022             <address>10.33.50.42</address>
3023             <port>1319</port>
3024         </destination>
3025         <protocol>tcp/udp</protocol>
3026         <target>192.168.13.19</target>
3027         <local-port>80</local-port>
3028         <interface>wan</interface>
3029         <descr><![CDATA[Port Forward to 192.168.13.19 Pf]]></descr>
3030         <associated-rule-id>nat_57c017e1e48d65.86612217</associated-rule-
3031 id>
3032         <updated>
3033             <time>1472206817</time>
3034             <username>admin@10.97.67.135</username>
3035         </updated>
3036         <created>
3037             <time>1472206817</time>
3038             <username>admin@10.97.67.135</username>
3039         </created>
3040     </rule>
3041     <rule>
3042         <source>
3043             <any/>
3044         </source>
3045         <destination>
3046             <address>10.33.50.42</address>
3047             <port>1320</port>
3048         </destination>
3049         <protocol>tcp/udp</protocol>
3050         <target>192.168.13.20</target>
3051         <local-port>80</local-port>
3052         <interface>wan</interface>
3053         <descr><![CDATA[Port Forward to 192.168.13.20 Pf]]></descr>
3054         <associated-rule-id>nat_57c0187fd4a074.12397754</associated-rule-
3055 id>
3056         <created>
3057             <time>1472206975</time>
3058             <username>admin@10.97.67.135</username>
3059         </created>

```

```

3060         <updated>
3061             <time>1477940348</time>
3062             <username>admin@192.168.13.139</username>
3063         </updated>
3064     </rule>
3065     <rule>
3066         <source>
3067             <any/>
3068         </source>
3069         <destination>
3070             <address>10.33.50.42</address>
3071             <port>2006</port>
3072         </destination>
3073         <protocol>tcp/udp</protocol>
3074         <target>192.168.20.6</target>
3075         <local-port>443</local-port>
3076         <interface>wan</interface>
3077         <descr><![CDATA[Port Forward to Hytrust Cloud Control
3078 192.168.20.6]]></descr>
3079         <associated-rule-id>nat_585ab274d8bce0.68941358</associated-rule-
3080 id>
3081         <updated>
3082             <time>1482338932</time>
3083             <username>admin@10.97.67.139</username>
3084         </updated>
3085         <created>
3086             <time>1482338932</time>
3087             <username>admin@10.97.67.139</username>
3088         </created>
3089     </rule>
3090     <separator/>
3091 </nat>
3092 <filter>
3093     <rule>
3094         <id/>
3095         <tracker>1483547179</tracker>
3096         <type>pass</type>
3097         <interface>enc0</interface>
3098         <ipprotocol>inet</ipprotocol>
3099         <tag/>

```

```

3100         <tagged/>
3101         <direction>any</direction>
3102         <quick>yes</quick>
3103         <floating>yes</floating>
3104         <max/>
3105         <max-src-nodes/>
3106         <max-src-conn/>
3107         <max-src-states/>
3108         <statetimeout/>
3109         <statetype>keep state</statetype>
3110         <os/>
3111         <source>
3112             <any/>
3113         </source>
3114         <destination>
3115             <any/>
3116         </destination>
3117         <descr><![CDATA[Allow IPSEC Traffic in both directions to
3118 pass]]></descr>
3119         <updated>
3120             <time>1483547179</time>
3121             <username>admin@10.97.67.165</username>
3122         </updated>
3123         <created>
3124             <time>1483547179</time>
3125             <username>admin@10.97.67.165</username>
3126         </created>
3127     </rule>
3128     <rule>
3129         <id/>
3130         <tracker>1481038469</tracker>
3131         <type>pass</type>
3132         <interface>lan</interface>
3133         <ipprotocol>inet</ipprotocol>
3134         <tag/>
3135         <tagged/>
3136         <direction>any</direction>
3137         <quick>yes</quick>
3138         <floating>yes</floating>
3139         <max/>

```



```

3140         <max-src-nodes/>
3141         <max-src-conn/>
3142         <max-src-states/>
3143         <statetimeout/>
3144         <statetype>keep state</statetype>
3145         <os/>
3146         <source>
3147             <address>192.168.14.111</address>
3148         </source>
3149         <destination>
3150             <any/>
3151         </destination>
3152         <descr><![CDATA[Allow Radiant (192.168.14.111) to go anywhere -
3153 LAN]]></descr>
3154         <updated>
3155             <time>1481038469</time>
3156             <username>admin@10.97.67.155</username>
3157         </updated>
3158         <created>
3159             <time>1481038469</time>
3160             <username>admin@10.97.67.155</username>
3161         </created>
3162     </rule>
3163     <rule>
3164         <id/>
3165         <tracker>1481134883</tracker>
3166         <type>pass</type>
3167         <interface>lan</interface>
3168         <ipprotocol>inet</ipprotocol>
3169         <tag/>
3170         <tagged/>
3171         <direction>any</direction>
3172         <quick>yes</quick>
3173         <floating>yes</floating>
3174         <max/>
3175         <max-src-nodes/>
3176         <max-src-conn/>
3177         <max-src-states/>
3178         <statetimeout/>
3179         <statetype>keep state</statetype>

```

```

3180         <os/>
3181         <source>
3182             <address>192.168.13.135</address>
3183         </source>
3184         <destination>
3185             <any/>
3186         </destination>
3187         <descr><![CDATA[Allow CA.acmefinancial to go anywhere]]></descr>
3188         <updated>
3189             <time>1481134883</time>
3190             <username>admin@10.97.67.146</username>
3191         </updated>
3192         <created>
3193             <time>1481134883</time>
3194             <username>admin@10.97.67.146</username>
3195         </created>
3196     </rule>
3197     <rule>
3198         <id/>
3199         <tracker>1481038517</tracker>
3200         <type>pass</type>
3201         <interface>lan</interface>
3202         <ipprotocol>inet</ipprotocol>
3203         <tag/>
3204         <tagged/>
3205         <direction>any</direction>
3206         <quick>yes</quick>
3207         <floating>yes</floating>
3208         <max/>
3209         <max-src-nodes/>
3210         <max-src-conn/>
3211         <max-src-states/>
3212         <statetimeout/>
3213         <statetype>keep state</statetype>
3214         <os/>
3215         <source>
3216             <address>192.168.17.100</address>
3217         </source>
3218         <destination>
3219             <any/>

```

## DRAFT

```
3220         </destination>
3221         <descr><![CDATA[Allow Radiant (192.168.17.100) to go anywhere -
3222 LAN]]></descr>
3223         <updated>
3224             <time>1481038517</time>
3225             <username>admin@10.97.67.155</username>
3226         </updated>
3227         <created>
3228             <time>1481038517</time>
3229             <username>admin@10.97.67.155</username>
3230         </created>
3231     </rule>
3232     <rule>
3233         <id/>
3234         <tracker>1478010422</tracker>
3235         <type>pass</type>
3236         <interface>wan</interface>
3237         <ipprotocol>inet</ipprotocol>
3238         <tag/>
3239         <tagged/>
3240         <direction>any</direction>
3241         <quick>yes</quick>
3242         <floating>yes</floating>
3243         <max/>
3244         <max-src-nodes/>
3245         <max-src-conn/>
3246         <max-src-states/>
3247         <statetimeout/>
3248         <statetype>keep state</statetype>
3249         <os/>
3250         <source>
3251             <any/>
3252         </source>
3253         <destination>
3254             <any/>
3255         </destination>
3256         <descr/>
3257         <updated>
3258             <time>1478010422</time>
3259             <username>admin@10.97.66.18</username>
```

```

3260         </updated>
3261         <created>
3262             <time>1478010422</time>
3263             <username>admin@10.97.66.18</username>
3264         </created>
3265     </rule>
3266     <rule>
3267         <id/>
3268         <tracker>1480540664</tracker>
3269         <type>pass</type>
3270         <interface>lan</interface>
3271         <ipprotocol>inet</ipprotocol>
3272         <tag/>
3273         <tagged/>
3274         <direction>any</direction>
3275         <quick>yes</quick>
3276         <floating>yes</floating>
3277         <max/>
3278         <max-src-nodes/>
3279         <max-src-conn/>
3280         <max-src-states/>
3281         <statetimeout/>
3282         <statetype>keep state</statetype>
3283         <os/>
3284         <source>
3285             <any/>
3286         </source>
3287         <destination>
3288             <any/>
3289         </destination>
3290         <descr><![CDATA[Allow all LAN traffic to go to anywhere]]></descr>
3291         <updated>
3292             <time>1480540664</time>
3293             <username>admin@10.97.67.140</username>
3294         </updated>
3295         <created>
3296             <time>1480540664</time>
3297             <username>admin@10.97.67.140</username>
3298         </created>
3299     </rule>

```

```

3300      <rule>
3301          <id/>
3302          <tracker>1472208251</tracker>
3303          <type>pass</type>
3304          <interface>lan</interface>
3305          <ipprotocol>inet</ipprotocol>
3306          <tag/>
3307          <tagged/>
3308          <direction>any</direction>
3309          <quick>yes</quick>
3310          <floating>yes</floating>
3311          <max/>
3312          <max-src-nodes/>
3313          <max-src-conn/>
3314          <max-src-states/>
3315          <statetimeout/>
3316          <statetype>keep state</statetype>
3317          <os/>
3318          <protocol>tcp/udp</protocol>
3319          <source>
3320              <address>192.168.0.0/16</address>
3321          </source>
3322          <destination>
3323              <address>192.168.0.0/16</address>
3324          </destination>
3325          <descr><![CDATA[Allow traffic going from local subnet to local
3326      subne]]></descr>
3327          <updated>
3328              <time>1472208251</time>
3329              <username>admin@10.97.67.135</username>
3330          </updated>
3331          <created>
3332              <time>1472208251</time>
3333              <username>admin@10.97.67.135</username>
3334          </created>
3335      </rule>
3336      <rule>
3337          <id/>
3338          <tracker>1472216936</tracker>
3339          <type>pass</type>

```

```

3340         <interface>lan</interface>
3341         <ipprotocol>inet</ipprotocol>
3342     </tag>
3343     <tagged/>
3344     <direction>any</direction>
3345     <quick>yes</quick>
3346     <floating>yes</floating>
3347     <max/>
3348     <max-src-nodes/>
3349     <max-src-conn/>
3350     <max-src-states/>
3351     <statetimeout/>
3352     <statetype>keep state</statetype>
3353     <os/>
3354     <protocol>tcp/udp</protocol>
3355     <source>
3356         <address>192.168.0.0/16</address>
3357     </source>
3358     <destination>
3359         <any/>
3360     </destination>
3361     <descr><![CDATA[Allow traffic going from local subnet to
3362 anywhere]]></descr>
3363     <updated>
3364         <time>1472216936</time>
3365         <username>admin@10.97.67.135</username>
3366     </updated>
3367     <created>
3368         <time>1472216936</time>
3369         <username>admin@10.97.67.135</username>
3370     </created>
3371 </rule>
3372 <rule>
3373     <id/>
3374     <tracker>1476720725</tracker>
3375     <type>pass</type>
3376     <interface>enc0</interface>
3377     <ipprotocol>inet</ipprotocol>
3378 </tag>
3379 <tagged/>

```

```

3380         <direction>any</direction>
3381         <quick>yes</quick>
3382         <floating>yes</floating>
3383         <max/>
3384         <max-src-nodes/>
3385         <max-src-conn/>
3386         <max-src-states/>
3387         <statetimeout/>
3388         <statetype>keep state</statetype>
3389         <os/>
3390         <source>
3391             <any/>
3392         </source>
3393         <destination>
3394             <any/>
3395         </destination>
3396         <descr><![CDATA[Allow All traffic sourced from Tunnel to Anywhere
3397 o]]></descr>
3398         <updated>
3399             <time>1476720725</time>
3400             <username>admin@10.97.67.137</username>
3401         </updated>
3402         <created>
3403             <time>1476720725</time>
3404             <username>admin@10.97.67.137</username>
3405         </created>
3406     </rule>
3407     <rule>
3408         <id/>
3409         <tracker>1471551236</tracker>
3410         <type>pass</type>
3411         <interface>wan</interface>
3412         <ipprotocol>inet</ipprotocol>
3413         <tag/>
3414         <tagged/>
3415         <max/>
3416         <max-src-nodes/>
3417         <max-src-conn/>
3418         <max-src-states/>
3419         <statetimeout/>

```

```

3420         <statetype>keep state</statetype>
3421     </os>
3422     <protocol>tcp/udp</protocol>
3423     <source>
3424         <any/>
3425     </source>
3426     <destination>
3427         <any/>
3428     </destination>
3429     <descr><![CDATA[Allow all TCP/UDP Traffic sourced from WAN
3430 interface]]></descr>
3431     <updated>
3432         <time>1471551236</time>
3433         <username>admin@10.97.67.136</username>
3434     </updated>
3435     <created>
3436         <time>1471551236</time>
3437         <username>admin@10.97.67.136</username>
3438     </created>
3439 </rule>
3440 <rule>
3441     <id/>
3442     <tracker>1470759134</tracker>
3443     <type>pass</type>
3444     <interface>wan</interface>
3445     <ipprotocol>inet</ipprotocol>
3446     <tag/>
3447     <tagged/>
3448     <max/>
3449     <max-src-nodes/>
3450     <max-src-conn/>
3451     <max-src-states/>
3452     <statetimeout/>
3453     <statetype>keep state</statetype>
3454     <os/>
3455     <protocol>tcp/udp</protocol>
3456     <source>
3457         <any/>
3458     </source>
3459     <destination>

```



```

3460             <network>(self)</network>
3461         </destination>
3462         <descr><![CDATA[Rule to allow connection to firewall -can be
3463 tighten]]></descr>
3464         <updated>
3465             <time>1470759134</time>
3466             <username>admin@192.168.13.135</username>
3467         </updated>
3468         <created>
3469             <time>1470759134</time>
3470             <username>admin@192.168.13.135</username>
3471         </created>
3472     </rule>
3473     <rule>
3474         <id/>
3475         <tracker>1461788221</tracker>
3476         <type>pass</type>
3477         <interface>wan</interface>
3478         <ipprotocol>inet</ipprotocol>
3479         <tag/>
3480         <tagged/>
3481         <max/>
3482         <max-src-nodes/>
3483         <max-src-conn/>
3484         <max-src-states/>
3485         <statetimeout/>
3486         <statetype>keep state</statetype>
3487         <os/>
3488         <protocol>tcp</protocol>
3489         <source>
3490             <any/>
3491         </source>
3492         <destination>
3493             <any/>
3494         </destination>
3495         <descr/>
3496         <updated>
3497             <time>1461788221</time>
3498             <username>admin@192.168.1.2</username>
3499         </updated>

```

```

3500         <created>
3501             <time>1461788221</time>
3502             <username>admin@192.168.1.2</username>
3503         </created>
3504     </rule>
3505     <rule>
3506         <id/>
3507         <tracker>1465934823</tracker>
3508         <type>pass</type>
3509         <interface>wan</interface>
3510         <ipprotocol>inet</ipprotocol>
3511         <tag/>
3512         <tagged/>
3513         <max/>
3514         <max-src-nodes/>
3515         <max-src-conn/>
3516         <max-src-states/>
3517         <statetimeout/>
3518         <statetype>keep state</statetype>
3519         <os/>
3520         <protocol>icmp</protocol>
3521         <source>
3522             <any/>
3523         </source>
3524         <destination>
3525             <any/>
3526         </destination>
3527         <descr><![CDATA[Easy Rule: Passed from Firewall Log
3528 View]]></descr>
3529         <created>
3530             <time>1465934786</time>
3531             <username>Easy Rule</username>
3532         </created>
3533         <updated>
3534             <time>1465934839</time>
3535             <username>admin@192.168.13.101</username>
3536         </updated>
3537     </rule>
3538     <rule>
3539         <source>

```

```

3540             <any/>
3541         </source>
3542     <interface>wan</interface>
3543     <protocol>tcp/udp</protocol>
3544     <destination>
3545         <address>192.168.19.11</address>
3546         <port>80</port>
3547     </destination>
3548     <descr><![CDATA[NAT Port forward to openldap; Add /phpldapadmin to
3549 address]]></descr>
3550     <associated-rule-id>nat_57bf0c96d083f4.07194849</associated-rule-
3551 id>
3552     <tracker>1472138390</tracker>
3553     <created>
3554         <time>1472138390</time>
3555         <username>NAT Port Forward</username>
3556     </created>
3557 </rule>
3558 <rule>
3559     <source>
3560         <any/>
3561     </source>
3562     <interface>wan</interface>
3563     <protocol>tcp/udp</protocol>
3564     <destination>
3565         <address>192.168.13.14</address>
3566         <port>80</port>
3567     </destination>
3568     <descr><![CDATA[NAT Port Forward to 192.168.13.14 Pf]]></descr>
3569     <associated-rule-id>nat_57c01545c247f0.43308393</associated-rule-
3570 id>
3571     <tracker>1472206149</tracker>
3572     <created>
3573         <time>1472206149</time>
3574         <username>NAT Port Forward</username>
3575     </created>
3576 </rule>
3577 <rule>
3578     <source>
3579         <any/>
3580     </source>

```

```

3581         <interface>wan</interface>
3582         <protocol>tcp/udp</protocol>
3583         <destination>
3584             <address>192.168.13.15</address>
3585             <port>80</port>
3586         </destination>
3587         <descr><![CDATA[NAT Port Forward to 192.168.13.15 Pf]]></descr>
3588         <associated-rule-id>nat_57c0163d6e2de9.62906352</associated-rule-
3589 id>
3590         <tracker>1472206397</tracker>
3591         <created>
3592             <time>1472206397</time>
3593             <username>NAT Port Forward</username>
3594         </created>
3595     </rule>
3596     <rule>
3597         <source>
3598             <any/>
3599         </source>
3600         <interface>wan</interface>
3601         <protocol>tcp/udp</protocol>
3602         <destination>
3603             <address>192.168.13.16</address>
3604             <port>80</port>
3605         </destination>
3606         <descr><![CDATA[NAT Port Forward to 192.168.13.16 Pf]]></descr>
3607         <associated-rule-id>nat_57c01682da98c4.72334719</associated-rule-
3608 id>
3609         <tracker>1472206466</tracker>
3610         <created>
3611             <time>1472206466</time>
3612             <username>NAT Port Forward</username>
3613         </created>
3614     </rule>
3615     <rule>
3616         <source>
3617             <any/>
3618         </source>
3619         <interface>wan</interface>
3620         <protocol>tcp/udp</protocol>

```

```

3621         <destination>
3622             <address>192.168.13.17</address>
3623             <port>80</port>
3624         </destination>
3625         <descr><![CDATA[NAT Port Forward to 192.168.13.17 Pf]]></descr>
3626         <associated-rule-id>nat_57c01787b4e891.75909166</associated-rule-
3627 id>
3628         <tracker>1472206727</tracker>
3629         <created>
3630             <time>1472206727</time>
3631             <username>NAT Port Forward</username>
3632         </created>
3633     </rule>
3634     <rule>
3635         <source>
3636             <any/>
3637         </source>
3638         <interface>wan</interface>
3639         <protocol>tcp/udp</protocol>
3640         <destination>
3641             <address>192.168.13.18</address>
3642             <port>80</port>
3643         </destination>
3644         <descr><![CDATA[NAT Port Forward to 192.168.13.18 Pf]]></descr>
3645         <associated-rule-id>nat_57c017be3dffaf1.16882401</associated-rule-
3646 id>
3647         <tracker>1472206782</tracker>
3648         <created>
3649             <time>1472206782</time>
3650             <username>NAT Port Forward</username>
3651         </created>
3652     </rule>
3653     <rule>
3654         <source>
3655             <any/>
3656         </source>
3657         <interface>wan</interface>
3658         <protocol>tcp/udp</protocol>
3659         <destination>
3660             <address>192.168.13.19</address>

```

```

3661         <port>80</port>
3662     </destination>
3663     <descr><![CDATA[NAT Port Forward to 192.168.13.19 Pf]]></descr>
3664     <associated-rule-id>nat_57c017e1e48d65.86612217</associated-rule-
3665 id>
3666     <tracker>1472206817</tracker>
3667     <created>
3668         <time>1472206817</time>
3669         <username>NAT Port Forward</username>
3670     </created>
3671 </rule>
3672 <rule>
3673     <source>
3674         <any/>
3675     </source>
3676     <interface>wan</interface>
3677     <protocol>tcp/udp</protocol>
3678     <destination>
3679         <address>192.168.13.20</address>
3680         <port>80</port>
3681     </destination>
3682     <descr><![CDATA[NAT Port Forward to 192.168.13.20 Pf]]></descr>
3683     <associated-rule-id>nat_57c0187fd4a074.12397754</associated-rule-
3684 id>
3685     <tracker>1472206975</tracker>
3686     <created>
3687         <time>1472206975</time>
3688         <username>NAT Port Forward</username>
3689     </created>
3690 </rule>
3691 <rule>
3692     <source>
3693         <any/>
3694     </source>
3695     <interface>wan</interface>
3696     <protocol>tcp/udp</protocol>
3697     <destination>
3698         <address>192.168.17.10</address>
3699         <port>8000</port>
3700     </destination>

```

```

3701         <descr><![CDATA[NAT Splunk port 8000 Web Interface]]></descr>
3702         <associated-rule-id>nat_57d825ba865df6.65796295</associated-rule-
3703 id>
3704         <tracker>1473783226</tracker>
3705         <created>
3706             <time>1473783226</time>
3707             <username>NAT Port Forward</username>
3708         </created>
3709     </rule>
3710     <rule>
3711         <source>
3712             <any/>
3713         </source>
3714         <interface>wan</interface>
3715         <protocol>tcp/udp</protocol>
3716         <destination>
3717             <address>192.168.19.11</address>
3718             <port>22</port>
3719         </destination>
3720         <descr><![CDATA[NAT Port forward to openldap; ]]></descr>
3721         <associated-rule-id>nat_57f555406f2de3.01889708</associated-rule-
3722 id>
3723         <tracker>1475695936</tracker>
3724         <created>
3725             <time>1475695936</time>
3726             <username>NAT Port Forward</username>
3727         </created>
3728     </rule>
3729     <rule>
3730         <source>
3731             <any/>
3732         </source>
3733         <interface>wan</interface>
3734         <protocol>tcp</protocol>
3735         <destination>
3736             <address>192.168.13.130</address>
3737             <port>80</port>
3738         </destination>
3739         <descr><![CDATA[NAT Mapping to pfsense 192.168.13.130]]></descr>
3740         <associated-rule-id>nat_581795efbc2944.51341500</associated-rule-
3741 id>

```

```

3742         <tracker>1477940719</tracker>
3743         <created>
3744             <time>1477940719</time>
3745             <username>NAT Port Forward</username>
3746         </created>
3747     </rule>
3748     <rule>
3749         <source>
3750             <any/>
3751         </source>
3752         <interface>wan</interface>
3753         <protocol>tcp/udp</protocol>
3754         <destination>
3755             <address>192.168.17.10</address>
3756             <port>22</port>
3757         </destination>
3758         <descr><![CDATA[NAT Splunk SSH ]]></descr>
3759         <associated-rule-id>nat_582ef78ed63d23.63868026</associated-rule-
3760 id>
3761         <tracker>1479473038</tracker>
3762         <created>
3763             <time>1479473038</time>
3764             <username>NAT Port Forward</username>
3765         </created>
3766     </rule>
3767     <rule>
3768         <source>
3769             <any/>
3770         </source>
3771         <interface>wan</interface>
3772         <protocol>tcp/udp</protocol>
3773         <destination>
3774             <address>192.168.20.6</address>
3775             <port>443</port>
3776         </destination>
3777         <descr><![CDATA[NAT Port Forward to Hytrust Cloud Control
3778 192.168.20.6]]></descr>
3779         <associated-rule-id>nat_585ab274d8bce0.68941358</associated-rule-
3780 id>
3781         <tracker>1482338932</tracker>
3782         <created>

```



```

3783             <time>1482338932</time>
3784             <username>NAT Port Forward</username>
3785         </created>
3786     </rule>
3787     <rule>
3788         <id/>
3789         <tracker>1480540738</tracker>
3790         <type>pass</type>
3791         <interface>lan</interface>
3792         <ipprotocol>inet</ipprotocol>
3793         <tag/>
3794         <tagged/>
3795         <max/>
3796         <max-src-nodes/>
3797         <max-src-conn/>
3798         <max-src-states/>
3799         <statetimeout/>
3800         <statetype>keep state</statetype>
3801         <os/>
3802         <source>
3803             <any/>
3804         </source>
3805         <destination>
3806             <any/>
3807         </destination>
3808         <descr><![CDATA[Allow all LAN traffic to go to anywhere]]></descr>
3809         <updated>
3810             <time>1480540738</time>
3811             <username>admin@10.97.67.140</username>
3812         </updated>
3813         <created>
3814             <time>1480540738</time>
3815             <username>admin@10.97.67.140</username>
3816         </created>
3817     </rule>
3818     <rule>
3819         <id/>
3820         <tracker>1465934857</tracker>
3821         <type>pass</type>
3822         <interface>lan</interface>

```

```

3823         <ipprotocol>inet</ipprotocol>
3824     </tag>
3825 </tagged/>
3826 </max/>
3827 </max-src-nodes/>
3828 </max-src-conn/>
3829 </max-src-states/>
3830 </statetimeout/>
3831 <statetype>keep state</statetype>
3832 </os/>
3833 <protocol>icmp</protocol>
3834 <source>
3835     <any/>
3836 </source>
3837 <destination>
3838     <any/>
3839 </destination>
3840 </descr/>
3841 <updated>
3842     <time>1465934857</time>
3843     <username>admin@192.168.13.101</username>
3844 </updated>
3845 <created>
3846     <time>1465934857</time>
3847     <username>admin@192.168.13.101</username>
3848 </created>
3849 </rule>
3850 <rule>
3851     <type>pass</type>
3852     <ipprotocol>inet</ipprotocol>
3853     <descr><![CDATA[Default allow LAN to any rule]]></descr>
3854     <interface>lan</interface>
3855     <tracker>0100000101</tracker>
3856     <source>
3857         <network>lan</network>
3858     </source>
3859     <destination>
3860         <any/>
3861     </destination>
3862 </rule>

```

```

3863         <rule>
3864             <type>pass</type>
3865             <ipprotocol>inet6</ipprotocol>
3866             <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
3867             <interface>lan</interface>
3868             <tracker>0100000102</tracker>
3869             <source>
3870                 <network>lan</network>
3871             </source>
3872             <destination>
3873                 <any/>
3874             </destination>
3875         </rule>
3876         <rule>
3877             <id/>
3878             <tracker>1476720530</tracker>
3879             <type>pass</type>
3880             <interface>enc0</interface>
3881             <ipprotocol>inet</ipprotocol>
3882             <tag/>
3883             <tagged/>
3884             <max/>
3885             <max-src-nodes/>
3886             <max-src-conn/>
3887             <max-src-states/>
3888             <statetimeout/>
3889             <statetype>keep state</statetype>
3890             <os/>
3891             <source>
3892                 <any/>
3893             </source>
3894             <destination>
3895                 <any/>
3896             </destination>
3897             <descr><![CDATA[Allow All traffic sourced from Tunnel to Anywhere
3898 o]]></descr>
3899             <created>
3900                 <time>1476720530</time>
3901                 <username>admin@10.97.67.137</username>
3902             </created>

```

```

3903             <updated>
3904                 <time>1476720628</time>
3905                 <username>admin@10.97.67.137</username>
3906             </updated>
3907         </rule>
3908         <separator>
3909             <lan/>
3910             <wan/>
3911             <floatingrules/>
3912             <enc0/>
3913         </separator>
3914         <bypassstaticroutes>yes</bypassstaticroutes>
3915     </filter>
3916     <shaper/>
3917     <ipsec>
3918         <phase1>
3919             <ikeid>1</ikeid>
3920             <iketype>ikev1</iketype>
3921             <mode>main</mode>
3922             <interface>wan</interface>
3923             <remote-gateway>174.47.13.99</remote-gateway>
3924             <protocol>inet</protocol>
3925             <myid_type>myaddress</myid_type>
3926             <myid_data/>
3927             <peerid_type>peeraddress</peerid_type>
3928             <peerid_data/>
3929             <encryption-algorithm>
3930                 <name>aes</name>
3931                 <keylen>256</keylen>
3932             </encryption-algorithm>
3933             <hash-algorithm>sha1</hash-algorithm>
3934             <dhgroup>2</dhgroup>
3935             <lifetime>28800</lifetime>
3936             <pre-shared-key>78J%3Akmp*Krr294xYE=v@</pre-shared-key>
3937             <private-key/>
3938             <certref/>
3939             <caref/>
3940             <authentication_method>pre_shared_key</authentication_method>
3941             <descr><![CDATA[IPSEC IKEv1 Tunnel to Vanguard's Firewall Public
3942 IP address]]></descr>

```

```

3943         <nat_traversal>force</nat_traversal>
3944         <mobike>off</mobike>
3945         <dpd_delay>10</dpd_delay>
3946         <dpd_maxfail>5</dpd_maxfail>
3947     </phase1>
3948     <client/>
3949     <phase2>
3950         <ikeid>1</ikeid>
3951         <uniqid>5804f45c4f196</uniqid>
3952         <mode>tunnel</mode>
3953         <reqid>1</reqid>
3954         <localid>
3955             <type>network</type>
3956             <address>192.168.19.0</address>
3957             <netbits>24</netbits>
3958         </localid>
3959         <remoteid>
3960             <type>network</type>
3961             <address>172.17.212.0</address>
3962             <netbits>24</netbits>
3963         </remoteid>
3964         <protocol>esp</protocol>
3965         <encryption-algorithm-option>
3966             <name>aes</name>
3967             <keylen>256</keylen>
3968         </encryption-algorithm-option>
3969         <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
3970         <pfsgroup>0</pfsgroup>
3971         <lifetime>3600</lifetime>
3972         <pinghost/>
3973         <descr><![CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
3974     </phase2>
3975     <phase2>
3976         <ikeid>1</ikeid>
3977         <uniqid>586d5ecf7f516</uniqid>
3978         <mode>tunnel</mode>
3979         <reqid>2</reqid>
3980         <localid>
3981             <type>network</type>
3982             <address>192.168.17.0</address>

```

```

3983         <netbits>24</netbits>
3984     </localid>
3985     <remoteid>
3986         <type>network</type>
3987         <address>172.17.212.0</address>
3988         <netbits>24</netbits>
3989     </remoteid>
3990     <protocol>esp</protocol>
3991     <encryption-algorithm-option>
3992         <name>aes</name>
3993         <keylen>256</keylen>
3994     </encryption-algorithm-option>
3995     <hash-algorithm-option>hmac_shal</hash-algorithm-option>
3996     <pfsgroup>0</pfsgroup>
3997     <lifetime>3600</lifetime>
3998     <pinghost/>
3999     <descr><![CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
4000 </phase2>
4001 <phase2>
4002     <ikeid>1</ikeid>
4003     <uniqid>586d5eeb02957</uniqid>
4004     <mode>tunnel</mode>
4005     <reqid>3</reqid>
4006     <localid>
4007         <type>network</type>
4008         <address>192.168.13.0</address>
4009         <netbits>24</netbits>
4010     </localid>
4011     <remoteid>
4012         <type>network</type>
4013         <address>172.17.212.0</address>
4014         <netbits>24</netbits>
4015     </remoteid>
4016     <protocol>esp</protocol>
4017     <encryption-algorithm-option>
4018         <name>aes</name>
4019         <keylen>256</keylen>
4020     </encryption-algorithm-option>
4021     <hash-algorithm-option>hmac_shal</hash-algorithm-option>
4022     <pfsgroup>0</pfsgroup>

```

```

4023         <lifetime>3600</lifetime>
4024         <pinghost/>
4025         <descr><![CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
4026     </phase2>
4027     <phase2>
4028         <ikeid>1</ikeid>
4029         <uniqid>586d5f54943b4</uniqid>
4030         <mode>tunnel</mode>
4031         <reqid>4</reqid>
4032         <localid>
4033             <type>network</type>
4034             <address>192.168.14.0</address>
4035             <netbits>24</netbits>
4036         </localid>
4037         <remoteid>
4038             <type>network</type>
4039             <address>172.17.212.0</address>
4040             <netbits>24</netbits>
4041         </remoteid>
4042         <protocol>esp</protocol>
4043         <encryption-algorithm-option>
4044             <name>aes</name>
4045             <keylen>256</keylen>
4046         </encryption-algorithm-option>
4047         <hash-algorithm-option>hmac_sha1</hash-algorithm-option>
4048         <pfsgroup>0</pfsgroup>
4049         <lifetime>3600</lifetime>
4050         <pinghost/>
4051         <descr><![CDATA[Phase 2 IPSEC Tunnel to Vanguard]]></descr>
4052     </phase2>
4053 </ipsec>
4054 <aliases/>
4055 <proxyarp/>
4056 <cron>
4057     <item>
4058         <minute>1,31</minute>
4059         <hour>0-5</hour>
4060         <mday>*</mday>
4061         <month>*</month>
4062         <wday>*</wday>

```

```

4063             <who>root</who>
4064             <command>/usr/bin/nice -n20 adjkerntz -a</command>
4065         </item>
4066         <item>
4067             <minute>1</minute>
4068             <hour>3</hour>
4069             <mday>1</mday>
4070             <month>*</month>
4071             <wday>*</wday>
4072             <who>root</who>
4073             <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
4074         </item>
4075         <item>
4076             <minute>*/60</minute>
4077             <hour>*</hour>
4078             <mday>*</mday>
4079             <month>*</month>
4080             <wday>*</wday>
4081             <who>root</who>
4082             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4083 sshlockout</command>
4084         </item>
4085         <item>
4086             <minute>*/60</minute>
4087             <hour>*</hour>
4088             <mday>*</mday>
4089             <month>*</month>
4090             <wday>*</wday>
4091             <who>root</who>
4092             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4093 webConfiguratorlockout</command>
4094         </item>
4095         <item>
4096             <minute>1</minute>
4097             <hour>1</hour>
4098             <mday>*</mday>
4099             <month>*</month>
4100             <wday>*</wday>
4101             <who>root</who>
4102             <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>

```



```

4103         </item>
4104         <item>
4105             <minute>*/60</minute>
4106             <hour>*</hour>
4107             <mday>*</mday>
4108             <month>*</month>
4109             <wday>*</wday>
4110             <who>root</who>
4111             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
4112 virusprot</command>
4113         </item>
4114         <item>
4115             <minute>30</minute>
4116             <hour>12</hour>
4117             <mday>*</mday>
4118             <month>*</month>
4119             <wday>*</wday>
4120             <who>root</who>
4121             <command>/usr/bin/nice -n20 /etc/rc.update_urldatales</command>
4122         </item>
4123     </cron>
4124     <wol/>
4125     <rrd>
4126         <enable/>
4127     </rrd>
4128     <load_balancer>
4129         <monitor_type>
4130             <name>ICMP</name>
4131             <type>icmp</type>
4132             <descr><![CDATA[ICMP]]></descr>
4133             <options/>
4134         </monitor_type>
4135         <monitor_type>
4136             <name>TCP</name>
4137             <type>tcp</type>
4138             <descr><![CDATA[Generic TCP]]></descr>
4139             <options/>
4140         </monitor_type>
4141         <monitor_type>
4142             <name>HTTP</name>

```

```

4143         <type>http</type>
4144         <descr><![CDATA[Generic HTTP]]></descr>
4145         <options>
4146             <path>/</path>
4147             <host/>
4148             <code>200</code>
4149         </options>
4150     </monitor_type>
4151     <monitor_type>
4152         <name>HTTPS</name>
4153         <type>https</type>
4154         <descr><![CDATA[Generic HTTPS]]></descr>
4155         <options>
4156             <path>/</path>
4157             <host/>
4158             <code>200</code>
4159         </options>
4160     </monitor_type>
4161     <monitor_type>
4162         <name>SMTP</name>
4163         <type>send</type>
4164         <descr><![CDATA[Generic SMTP]]></descr>
4165         <options>
4166             <send/>
4167             <expect>220 *</expect>
4168         </options>
4169     </monitor_type>
4170 </load_balancer>
4171 <widgets>
4172     <sequence>system_information:coll:open,gateways:coll:open,interfaces:col2:open<
4173 /sequence>
4174 </widgets>
4175 <openvpn/>
4176 <dnshaper/>
4177 <unbound>
4178     <enable/>
4179     <dnssec/>
4180     <active_interface/>
4181     <outgoing_interface/>
4182     <custom_options/>

```

```

4184         <hideidentity/>
4185         <hideversion/>
4186         <dnssecstripped/>
4187     </unbound>
4188     <dhcpdv6>
4189         <lan>
4190             <range>
4191                 <from>::1000</from>
4192                 <to>::2000</to>
4193             </range>
4194             <ramode>assist</ramode>
4195             <rapriority>medium</rapriority>
4196         </lan>
4197     </dhcpdv6>
4198     <cert>
4199         <refid>5720a0502b277</refid>
4200         <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
4201         <type>server</type>
4202     </cert>
4203     <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXZ0F3SUJBZ0lCQURBTk1Jna3
4204 Foa2lHOXcwQkFRc0ZBRENCdERFTE1Ba0dBmVVFQmhnQ1ZWtXGKRGPBTUJnTlZCQWdUQ1ZOMFlYUmXNUkV3RHdZ
4205 RFZRUUhFd2hNYjJOaGJHbDBlVEU0TURZR0ExVUVDaE12Y0daVApaVzV6WlNCM1pXSkrImjVtYVdkMWNtRjBiM0
4206 lnVTJWc1ppMVRhV2R1WldRZlEyVnlkR2xtYVd0aGRHVXhLREFTcKJna3Foa2lHOXcwQkNRRVdHV0ZrYldsVFI
4207 Qm1VM1ZlYzJVdWJHOWpZV3hrYjIxaGFxNhhIakFjQmdOVk1JBTBTVQKRlhCbVUyVnVjM1V0TlRjeU1HRXdoVEF5WW
4208 pJM056QWVGdzB4TmBME1qY3hNVEU1TkRSYU1TlZCQWNUCkNFeHZZMkZzYVhSNu1UZ3d0Z1lEVlFRS0
4209 d0pWVXpFT01Bd0dBmVVFQ0JNR1UzUmhkR1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNu1UZ3d0Z1lEVlFRS0
4210 V5OXdaE5sYm5ObElIZGxZa052YmlacFozVnlZWFFJ2Y21CVFpXeg0KTFZ0cFoyNWxaQ0JEWlhKMGFxWnBZMkYw
4211 WlRfb01DWUdDU3FHu01iM0RRRUUpBU1laWVdSdGFxNUFjR1pUW1cllegpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
4212 dBmVVFQXhNVMNHWlRaVzV6WlMwMU56SXdZVEExTURKaU1qYzNNSU1CCk1qQU5CZ2txaGtpRz13MEJBuUUGQUFP
4213 Q0FROEFNSU1CQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
4214 hDODBU0dhZnJENWdqctRwZkNNMH1zbEFPaV1ZK1hdyjdNa2o0dmtTMgpmBz14emNyaDUrNV1aYlBHEXR1a21s
4215 ZWR4bjFwEFl6S1l1ZXZkdnlKb1lRMCTntKx0dkFjYnRhTUfoZjh1ZkRfClhrc1NVQ0N5YTFrbEYxNWJGZmcyUg
4216 E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkJFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKZzh
4217 ZEFiUEhjWgc5SFA0NFQybfFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXdlSEZwd3J1LytYWExieEcrcD
4218 dwYXI0aHR0UFRDcm1lNmFqQVVTNmpvN05kOE1QNWpZ1kzR0h2Zjh1ZkRfClhrc1NVQ0N5YTFrbEYxNWJGZmcyUg
4219 V1IwVEJBSXdBREFSQmdsZ2hrZ0JodmhDQVFFRUJBTUNCa0F3TXdZS1lJWkkKQV1iNFfFRU5CQ1lXSku5d1pXNV
4220 RVMHdnUjJWdVpYSmhkr1ZrSUZ0bGNuWmxjaUJEWlhKMGFxWnBZMkYwWlRbZApCZ05WSFE0RUZnUVU3K1lLRmNp
4221 OFFVSGhTZ0xEdjhfQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RdQjFvQVU3K1lLcKZjaThRVUhoU2dMRHY4RUNzY0
4222 NKd0FLaGdicWtnYmN3Z2JREnE6QUpCZ05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0EX
4223 VUVCeE1JVEc5allXeHBkSGt4T0RBMk1JnTlZCQW9UTDNCbVUyVnVjM1VnZDJWaqPmJ1lWm1sbmRYSmhkrZ15SU
4224 ZObGJHXRVMmxYm1Wa0lFTmxjblJwWm1sallYUmXNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
4225 bE5sYm5ObExtEHZZMkZzWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhnRFV3TW1JeU
4226 56ZUNBUUF3SFFZRFZSMGxCQ1l3RkFZSut3WUJCUVVIQXdfR0NDc0dBuVVGQ0FJQWpNQXNHQTFVZER3SUUVBd01G
4227 b0RBTk1Jna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZfPQdXd2MVZuUC82NmJDFWJ5CkVmaW1LRW1PcmntNaTB5M0
4228 9PWGtzWes1cEM2dtd6Ukl3WjEvRjYyRUp3OD1UOWx4Y01ZelZOTm5Idlg0bXFPURcKUWJhRU42NEkxOHFud3Zm
4229 S2JrREZvRThMR1hSdzBkMnAyTGMvYU1Td4YTIvSGNHc0xHTktPbkjXb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG
4230 c4bGdrcVc3dStlb01DNDJlBvJkOURCTm1zdfFJ4RVLNMkFLQkFsZG1LYStvRUy1VUwwCm43aXpvN1Z4dHJWMTJv
4231 TTdyS1lRQ05ky00xZkVSeUwvb3ZkUnVpa0F5Wm1VvNfULldDZGo3dDdIVG9ob0RFYzEKSklkOvpPSmR2QmZLVU
4232 1sUW1ELyswSvpTalFXRDczWkdsEhTK2tOeWcladJhUjUwYjh3Wm9zQnNjSUZDa0pFbgp0UT09Ci0tLS0tRU5E
4233 IENFU1RJRklDQVRFLS0tLS0K</crt>
4234
4235     <prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z0lCQURBTk1Jna3Foa2lHOXcwQkFRRU
4236 ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M01hY1lkMjN3YkNKR1htWFJWky9odVVKefDsc3hxb3M4

```

```

4237 eGxiY3UyRUx6UVpJWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMWitqM0hOeXVibjdsaGxzOG
4238 JLMjZTS1Y1M0dmVlhGak1saXhxOG0vSW1oaERUNHcWdTI4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEpyV1NVWFhs
4239 c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcWdkEKQVdEQkQzNDg5OHRUa1hROVNPb1Nac1REbn
4240 dKTmo3cHAWQnM4ZHh1RDBjL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
4241 dHZFYjZudWxxdm1HMjA5TUt1SzdwU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUpRRF
4242 pxU3duMnNTUTh0SVNBTVUvUW0zcXhrb3BzdZB4cWNScmF0Ed4VmQKejBpOU1KbkZVQWFleTQvL3JldndhZW1P
4243 R3RYSmZ2ai9jSnY3cmJIWGIzYkTjVW9hcDhxY0RjdVSMmlHRUZyWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcD
4244 lzNVhchHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQX4dSGJZWWhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1Zn1P
4245 UzAvbXlmNU5YLzVoRklPNmFDc0xlUjZ4N1RZa2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
4246 hMZ0NRY1B2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtwNzhMY1FPMgppsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
4247 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUe0NzNMUWoxcExLSmRZN2JxCmtMU3NVt0ZhTUZlZG1xU2ttbzh3Qj
4248 lpMXhzbElLQUd0M3U4dTdMz1ZtU2lybnMwVVBtMHRVUDRyQXMzVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
4249 OGttbFJnUFRmVHVPaGNgMGVkamQwK1E5Y2V1Y25kaFp3UEl6TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHNhbm
4250 NBRDhVYThDZ1l1FQXpzYjYzbzRBSH1YNjZkEJ6TG1zYzZxS2d2ZG4xazhVCm02N3RuK2M3NkVhSEtZT1k0Rjdh
4251 S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSX4d5cUx5T1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUOK0I3Sm
4252 Z2RjYrK2tHa1NHOGxaN0VLY2lUc1kzRVJxOURsSk94Nk1ROFEwMDNsThVtQQpJZmlDWlpRSUQ1OENnWUJjamFO
4253 dk5obnFJOG9rWGhBUjR2c3NtNgPwb0tYU1ZScjRIVHo5MDfWOGdReXNCWkt0CnlUS2V6VThuUVZvTjNYWmVMbC
4254 8rVEcwYVpKOTZHKy9nNTRWZmZqWTRlelVSChhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
4255 QWY5Mi9CbHZJR25FS1pMdnhLWTdVMX1Ib1NRLzczUG1D5nFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
4256 VudmNUUjZxTzR0ekZtdG5TYWN3W1Ftb2UvdUVIaE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
4257 RG1hZGsvKy9Ud2UvVk1KbmX2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUj1hbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
4258 FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBR50JnQ0xDR0R1RXNBYUxwZ1RtOG44bgoyQ1h1NE52K1l3a1RlcZdu
4259 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGdlp3cC9uSVdycnRCZlZLClUzStShhYnpnUUtWOEwrZj
4260 VadTAXY1pZVvK5TU0FIUFRHYm5jb1IzbGVpYjNleUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
4261 OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>
4262 </cert>
4263 <revision>
4264 <time>1493217875</time>
4265 <description><![CDATA[admin@10.97.67.148: /firewall_nat_1to1_edit.php
4266 made unknown change]]></description>
4267 <username>admin@10.97.67.148</username>
4268 </revision>
4269 <gateways>
4270 <gateway_item>
4271 <interface>wan</interface>
4272 <gateway>10.33.50.33</gateway>
4273 <name>GW_WAN</name>
4274 <weight>1</weight>
4275 <ipprotocol>inet</ipprotocol>
4276 <interval/>
4277 <descr><![CDATA[Interface wan Gateway]]></descr>
4278 <defaultgw/>
4279 </gateway_item>
4280 <gateway_item>
4281 <interface>lan</interface>
4282 <gateway>192.168.13.14</gateway>
4283 <name>VLAN2014</name>
4284 <weight>1</weight>
4285 <ipprotocol>inet</ipprotocol>

```

```

4286         <descr/>
4287     </gateway_item>
4288     <gateway_item>
4289         <interface>lan</interface>
4290         <gateway>192.168.13.19</gateway>
4291         <name>VLAN2019</name>
4292         <weight>1</weight>
4293         <ipprotocol>inet</ipprotocol>
4294         <descr><![CDATA[VLAN2019]]></descr>
4295     </gateway_item>
4296     <gateway_item>
4297         <interface>lan</interface>
4298         <gateway>192.168.13.18</gateway>
4299         <name>VLAN2018</name>
4300         <weight>1</weight>
4301         <ipprotocol>inet</ipprotocol>
4302         <descr><![CDATA[VLAN2018]]></descr>
4303     </gateway_item>
4304     <gateway_item>
4305         <interface>lan</interface>
4306         <gateway>192.168.13.15</gateway>
4307         <name>VLAN2015</name>
4308         <weight>1</weight>
4309         <ipprotocol>inet</ipprotocol>
4310         <descr/>
4311     </gateway_item>
4312     <gateway_item>
4313         <interface>lan</interface>
4314         <gateway>192.168.13.16</gateway>
4315         <name>VLAN2016</name>
4316         <weight>1</weight>
4317         <ipprotocol>inet</ipprotocol>
4318         <descr/>
4319     </gateway_item>
4320     <gateway_item>
4321         <interface>lan</interface>
4322         <gateway>192.168.13.17</gateway>
4323         <name>VLAN2017</name>
4324         <weight>1</weight>
4325         <ipprotocol>inet</ipprotocol>

```

```

4326             <descr/>
4327         </gateway_item>
4328         <gateway_item>
4329             <interface>lan</interface>
4330             <gateway>192.168.13.20</gateway>
4331             <name>VLAN2020</name>
4332             <weight>1</weight>
4333             <ipprotocol>inet</ipprotocol>
4334             <descr/>
4335         </gateway_item>
4336         <gateway_item>
4337             <interface>lan</interface>
4338             <gateway>192.168.13.10</gateway>
4339             <name>VLAN2066</name>
4340             <weight>1</weight>
4341             <ipprotocol>inet</ipprotocol>
4342             <descr><![CDATA[Gateway to Vendor Net]]></descr>
4343         </gateway_item>
4344     </gateways>
4345     <ppps/>
4346     <dyndnses/>
4347     <virtualip>
4348         <vip>
4349             <mode>ipalias</mode>
4350             <interface>wan</interface>
4351             <uniqid>576b23658af3d</uniqid>
4352             <descr><![CDATA[Virtual IP for Splunk]]></descr>
4353             <type>single</type>
4354             <subnet_bits>32</subnet_bits>
4355             <subnet>10.33.50.35</subnet>
4356         </vip>
4357         <vip>
4358             <mode>ipalias</mode>
4359             <interface>wan</interface>
4360             <uniqid>5773d4c39ae54</uniqid>
4361             <descr><![CDATA[Virtual IP for RadiantOne VDS]]></descr>
4362             <type>single</type>
4363             <subnet_bits>32</subnet_bits>
4364             <subnet>10.33.50.37</subnet>
4365         </vip>

```

```

4366      <vip>
4367          <mode>ipalias</mode>
4368          <interface>wan</interface>
4369          <uniqid>57a8ce7868f78</uniqid>
4370          <descr><![CDATA[Virtual IP for Hytrust ESXi Server]]></descr>
4371          <type>single</type>
4372          <subnet_bits>32</subnet_bits>
4373          <subnet>10.33.50.36</subnet>
4374      </vip>
4375      <vip>
4376          <mode>ipalias</mode>
4377          <interface>wan</interface>
4378          <uniqid>57aa0a09a4d09</uniqid>
4379          <descr><![CDATA[VIP for Hytrust CloudControl VM]]></descr>
4380          <type>single</type>
4381          <subnet_bits>32</subnet_bits>
4382          <subnet>10.33.50.38</subnet>
4383      </vip>
4384      <vip>
4385          <mode>ipalias</mode>
4386          <interface>wan</interface>
4387          <uniqid>57b615eac1f16</uniqid>
4388          <descr><![CDATA[VIP for VCenter Server]]></descr>
4389          <type>single</type>
4390          <subnet_bits>32</subnet_bits>
4391          <subnet>10.33.50.39</subnet>
4392      </vip>
4393      <vip>
4394          <mode>ipalias</mode>
4395          <interface>wan</interface>
4396          <uniqid>57bd089e9ab62</uniqid>
4397          <descr><![CDATA[VIP for ActiveDirectory]]></descr>
4398          <type>single</type>
4399          <subnet_bits>32</subnet_bits>
4400          <subnet>10.33.50.40</subnet>
4401      </vip>
4402      <vip>
4403          <mode>ipalias</mode>
4404          <interface>wan</interface>
4405          <uniqid>57bf0bbc594c5</uniqid>

```

```

4406         <descr><![CDATA[VIP for OpenLDAP]]></descr>
4407         <type>single</type>
4408         <subnet_bits>32</subnet_bits>
4409         <subnet>10.33.50.41</subnet>
4410     </vip>
4411     <vip>
4412         <mode>ipalias</mode>
4413         <interface>wan</interface>
4414         <uniqid>57bf97481ae8c</uniqid>
4415         <descr><![CDATA[VIP for Internal Pfsense Firewalls]]></descr>
4416         <type>single</type>
4417         <subnet_bits>32</subnet_bits>
4418         <subnet>10.33.50.42</subnet>
4419     </vip>
4420     <vip>
4421         <mode>ipalias</mode>
4422         <interface>wan</interface>
4423         <uniqid>581788c622d42</uniqid>
4424         <descr><![CDATA[VIP for ConsoleWorks -- Mapping to Internal
4425 Address]]></descr>
4426         <type>single</type>
4427         <subnet_bits>32</subnet_bits>
4428         <subnet>10.33.50.43</subnet>
4429     </vip>
4430     <vip>
4431         <mode>ipalias</mode>
4432         <interface>wan</interface>
4433         <uniqid>58179833f127e</uniqid>
4434         <descr><![CDATA[Testing ]]></descr>
4435         <type>single</type>
4436         <subnet_bits>32</subnet_bits>
4437         <subnet>10.33.50.44</subnet>
4438     </vip>
4439     <vip>
4440         <mode>ipalias</mode>
4441         <interface>wan</interface>
4442         <uniqid>58e410a9241f1</uniqid>
4443         <descr><![CDATA[Mapping to CentOSToAD VM (test machine)]]></descr>
4444         <type>single</type>
4445         <subnet_bits>32</subnet_bits>

```



```

4446         <subnet>10.33.50.45</subnet>
4447     </vip>
4448     <vip>
4449         <mode>ipalias</mode>
4450         <interface>wan</interface>
4451         <uniqid>5900b1ef3b079</uniqid>
4452         <descr><![CDATA[AlertEnterprise Enterprise Guardian]]></descr>
4453         <type>single</type>
4454         <subnet_bits>32</subnet_bits>
4455         <subnet>10.33.50.46</subnet>
4456     </vip>
4457 </virtualip>
4458 </pfSense>

```

## 2.10.2 Firewall Configuration for Common Services Subnet

```

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

```

```

4485         <name>admin</name>
4486         <descr><![CDATA[System Administrator]]></descr>
4487         <scope>system</scope>
4488         <groupname>admins</groupname>
4489         <password>$1$dSJmFph$GvZ7.1UbuWu.Yb8etC0re.</password>
4490         <uid>0</uid>
4491         <priv>user-shell-access</priv>
4492     </user>
4493     <nextuid>2000</nextuid>
4494     <nextgid>2000</nextgid>
4495     <timezone>America/New_York</timezone>
4496     <time-update-interval/>
4497     <timeservers>10.97.74.8</timeservers>
4498     <webgui>
4499         <protocol>http</protocol>
4500         <loginautocomplete/>
4501         <ssl-certref>5720a0502b277</ssl-certref>
4502         <dashboardcolumns>2</dashboardcolumns>
4503         <port/>
4504         <max_procs>2</max_procs>
4505         <nohttppreferercheck/>
4506     </webgui>
4507     <disablenatreflection>yes</disablenatreflection>
4508     <disablesegmentationoffloading/>
4509     <disablelargereceiveoffloading/>
4510     <ipv6allow/>
4511     <powerd_ac_mode>hadp</powerd_ac_mode>
4512     <powerd_battery_mode>hadp</powerd_battery_mode>
4513     <powerd_normal_mode>hadp</powerd_normal_mode>
4514     <bogons>
4515         <interval>monthly</interval>
4516     </bogons>
4517     <language>en_US</language>
4518     <dns1gw>GW_WAN</dns1gw>
4519     <dns2gw>GW_WAN</dns2gw>
4520     <dns3gw>none</dns3gw>
4521     <dns4gw>none</dns4gw>
4522     <dnsserver>10.97.74.8</dnsserver>
4523     <dnsserver>10.63.255.2</dnsserver>
4524     <maximumstates/>

```

```

4525         <aliasesresolveinterval/>
4526         <maximumtableentries/>
4527         <maximumfrags/>
4528         <reflectiontimeout/>
4529         <serialspeed>115200</serialspeed>
4530         <primaryconsole>serial</primaryconsole>
4531     </system>
4532     <interfaces>
4533         <wan>
4534             <if>em0</if>
4535             <descr><![CDATA[WAN]]></descr>
4536             <enable/>
4537             <spoofmac/>
4538             <ipaddr>192.168.13.19</ipaddr>
4539             <subnet>24</subnet>
4540             <gateway>GW_WAN_2</gateway>
4541             <ipaddrv6/>
4542             <subnetv6/>
4543             <gatewayv6/>
4544         </wan>
4545         <lan>
4546             <enable/>
4547             <if>em1</if>
4548             <ipaddr>192.168.19.1</ipaddr>
4549             <subnet>24</subnet>
4550             <ipaddrv6/>
4551             <subnetv6/>
4552             <media/>
4553             <mediaopt/>
4554             <track6-interface>wan</track6-interface>
4555             <track6-prefix-id>0</track6-prefix-id>
4556             <gateway/>
4557             <gatewayv6/>
4558         </lan>
4559     </interfaces>
4560     <staticroutes>
4561         <route>
4562             <network>192.168.17.0/24</network>
4563             <gateway>GW_VLAN17</gateway>
4564             <descr><![CDATA[Route to VLAN 17]]></descr>

```

```

4565         </route>
4566     </staticroutes>
4567     <dhcpd>
4568         <lan>
4569             <enable/>
4570             <range>
4571                 <from>192.168.19.100</from>
4572                 <to>192.168.19.150</to>
4573             </range>
4574         </lan>
4575         <opt1>
4576             <enable/>
4577             <range>
4578                 <from>192.168.14.100</from>
4579                 <to>192.168.14.150</to>
4580             </range>
4581         </opt1>
4582         <opt2>
4583             <enable/>
4584             <range>
4585                 <from>192.168.15.100</from>
4586                 <to>192.168.15.150</to>
4587             </range>
4588         </opt2>
4589         <opt3>
4590             <enable/>
4591             <range>
4592                 <from>192.168.16.100</from>
4593                 <to>192.168.16.150</to>
4594             </range>
4595         </opt3>
4596     </dhcpd>
4597     <snmpd>
4598         <syslocation/>
4599         <syscontact/>
4600         <rocommunity>public</rocommunity>
4601     </snmpd>
4602     <diag>
4603         <ipv6nat>
4604             <ipaddr/>

```

```

4605         </ipv6nat>
4606     </diag>
4607     <bridge/>
4608     <syslog/>
4609     <nat>
4610         <outbound>
4611             <mode>disabled</mode>
4612         </outbound>
4613     </nat>
4614     <filter>
4615         <rule>
4616             <id/>
4617             <tracker>1493319263</tracker>
4618             <type>pass</type>
4619             <interface>wan</interface>
4620             <ipprotocol>inet</ipprotocol>
4621             <tag/>
4622             <tagged/>
4623             <direction>any</direction>
4624             <quick>yes</quick>
4625             <floating>yes</floating>
4626             <max/>
4627             <max-src-nodes/>
4628             <max-src-conn/>
4629             <max-src-states/>
4630             <statetimeout/>
4631             <statetype>keep state</statetype>
4632             <os/>
4633             <protocol>tcp/udp</protocol>
4634             <source>
4635                 <any/>
4636             </source>
4637             <destination>
4638                 <network>lan</network>
4639             </destination>
4640             <descr><![CDATA[Allow Any to LAN net]]></descr>
4641             <updated>
4642                 <time>1493319263</time>
4643                 <username>admin@10.97.67.143</username>
4644             </updated>

```

```

4645         <created>
4646             <time>1493319263</time>
4647             <username>admin@10.97.67.143</username>
4648         </created>
4649         <disabled/>
4650     </rule>
4651     <rule>
4652         <id/>
4653         <tracker>1481038226</tracker>
4654         <type>pass</type>
4655         <interface>wan</interface>
4656         <ipprotocol>inet</ipprotocol>
4657         <tag/>
4658         <tagged/>
4659         <direction>any</direction>
4660         <quick>yes</quick>
4661         <floating>yes</floating>
4662         <max/>
4663         <max-src-nodes/>
4664         <max-src-conn/>
4665         <max-src-states/>
4666         <statetimeout/>
4667         <statetype>keep state</statetype>
4668         <os/>
4669         <source>
4670             <address>192.168.14.111</address>
4671         </source>
4672         <destination>
4673             <any/>
4674         </destination>
4675         <disabled/>
4676         <descr><![CDATA[Allow Radiant (192.168.14.111) in -WAN]]></descr>
4677         <created>
4678             <time>1481038226</time>
4679             <username>admin@10.97.67.155</username>
4680         </created>
4681         <updated>
4682             <time>1493311659</time>
4683             <username>admin@10.97.67.143</username>
4684         </updated>

```

```

4685         </rule>
4686     <rule>
4687         <id/>
4688         <tracker>1481038269</tracker>
4689         <type>pass</type>
4690         <interface>wan</interface>
4691         <ipprotocol>inet</ipprotocol>
4692         <tag/>
4693         <tagged/>
4694         <direction>any</direction>
4695         <quick>yes</quick>
4696         <floating>yes</floating>
4697         <max/>
4698         <max-src-nodes/>
4699         <max-src-conn/>
4700         <max-src-states/>
4701         <statetimeout/>
4702         <statetype>keep state</statetype>
4703         <os/>
4704         <protocol>tcp/udp</protocol>
4705         <source>
4706             <any/>
4707         </source>
4708         <destination>
4709             <network>lan</network>
4710             <port>389</port>
4711         </destination>
4712         <descr><![CDATA[Allow LDAP traffic to AD and OpenLDAP]]></descr>
4713         <created>
4714             <time>1481038269</time>
4715             <username>admin@10.97.67.155</username>
4716         </created>
4717         <updated>
4718             <time>1493319675</time>
4719             <username>admin@10.97.67.143</username>
4720         </updated>
4721     </rule>
4722 </rule>
4723     <id/>
4724     <tracker>1493314739</tracker>

```

```

4725         <type>pass</type>
4726         <interface>wan</interface>
4727         <ipprotocol>inet</ipprotocol>
4728         <tag/>
4729         <tagged/>
4730         <direction>any</direction>
4731         <quick>yes</quick>
4732         <floating>yes</floating>
4733         <max/>
4734         <max-src-nodes/>
4735         <max-src-conn/>
4736         <max-src-states/>
4737         <statetimeout/>
4738         <statetype>keep state</statetype>
4739         <os/>
4740         <protocol>tcp/udp</protocol>
4741         <source>
4742             <any/>
4743         </source>
4744         <destination>
4745             <any/>
4746             <port>636</port>
4747         </destination>
4748         <descr><![CDATA[Allow Connection to LDAPS on AD and
4749 OpenLDAP]]></descr>
4750         <created>
4751             <time>1493314739</time>
4752             <username>admin@10.97.67.143</username>
4753         </created>
4754         <updated>
4755             <time>1493319543</time>
4756             <username>admin@10.97.67.143</username>
4757         </updated>
4758     </rule>
4759     <rule>
4760         <id/>
4761         <tracker>1472179541</tracker>
4762         <type>pass</type>
4763         <interface>wan</interface>
4764         <ipprotocol>inet</ipprotocol>

```



```

4765         <tag/>
4766         <tagged/>
4767         <direction>any</direction>
4768         <quick>yes</quick>
4769         <floating>yes</floating>
4770         <max/>
4771         <max-src-nodes/>
4772         <max-src-conn/>
4773         <max-src-states/>
4774         <statetimeout/>
4775         <statetype>keep state</statetype>
4776         <os/>
4777         <protocol>tcp/udp</protocol>
4778         <source>
4779             <any/>
4780         </source>
4781         <destination>
4782             <any/>
4783         </destination>
4784         <disabled/>
4785         <descr><![CDATA[Testing to see if there will be communication
4786 between]]></descr>
4787         <created>
4788             <time>1472179541</time>
4789             <username>admin@192.168.13.135</username>
4790         </created>
4791         <updated>
4792             <time>1493311684</time>
4793             <username>admin@10.97.67.143</username>
4794         </updated>
4795     </rule>
4796     <rule>
4797         <id/>
4798         <tracker>1493327079</tracker>
4799         <type>pass</type>
4800         <interface>wan</interface>
4801         <ipprotocol>inet</ipprotocol>
4802         <tag/>
4803         <tagged/>
4804         <direction>any</direction>

```

```

4805         <quick>yes</quick>
4806         <floating>yes</floating>
4807         <max/>
4808         <max-src-nodes/>
4809         <max-src-conn/>
4810         <max-src-states/>
4811         <statetimeout/>
4812         <statetype>keep state</statetype>
4813         <os/>
4814         <protocol>icmp</protocol>
4815         <source>
4816             <any/>
4817         </source>
4818         <destination>
4819             <network>lan</network>
4820         </destination>
4821         <descr><![CDATA[Allow ICMP for troubleshooting]]></descr>
4822         <updated>
4823             <time>1493327079</time>
4824             <username>admin@10.97.67.143</username>
4825         </updated>
4826         <created>
4827             <time>1493327079</time>
4828             <username>admin@10.97.67.143</username>
4829         </created>
4830     </rule>
4831     <rule>
4832         <id/>
4833         <tracker>1493327306</tracker>
4834         <type>pass</type>
4835         <interface>wan</interface>
4836         <ipprotocol>inet</ipprotocol>
4837         <tag/>
4838         <tagged/>
4839         <direction>any</direction>
4840         <quick>yes</quick>
4841         <floating>yes</floating>
4842         <max/>
4843         <max-src-nodes/>
4844         <max-src-conn/>

```

```

4845         <max-src-states/>
4846         <statetimeout/>
4847         <statetype>keep state</statetype>
4848         <os></os>
4849         <protocol>tcp/udp</protocol>
4850         <source>
4851             <any/>
4852         </source>
4853         <destination>
4854             <any/>
4855             <port>53</port>
4856         </destination>
4857         <descr><![CDATA[Allow DNS Requests to AD]]></descr>
4858         <updated>
4859             <time>1493327306</time>
4860             <username>admin@10.97.67.143</username>
4861         </updated>
4862         <created>
4863             <time>1493327306</time>
4864             <username>admin@10.97.67.143</username>
4865         </created>
4866     </rule>
4867     <rule>
4868         <id/>
4869         <tracker>1493312171</tracker>
4870         <type>pass</type>
4871         <interface>wan</interface>
4872         <ipprotocol>inet</ipprotocol>
4873         <tag/>
4874         <tagged/>
4875         <max/>
4876         <max-src-nodes/>
4877         <max-src-conn/>
4878         <max-src-states/>
4879         <statetimeout/>
4880         <statetype>keep state</statetype>
4881         <os/>
4882         <protocol>tcp</protocol>
4883         <source>
4884             <any/>

```

```

4885         </source>
4886         <destination>
4887             <network>lan</network>
4888             <port>389</port>
4889         </destination>
4890         <descr><![CDATA[Allow LDAP traffic to LAN nodes]]></descr>
4891         <updated>
4892             <time>1493312171</time>
4893             <username>admin@10.97.67.143</username>
4894         </updated>
4895         <created>
4896             <time>1493312171</time>
4897             <username>admin@10.97.67.143</username>
4898         </created>
4899     </rule>
4900     <rule>
4901         <id/>
4902         <tracker>1493313314</tracker>
4903         <type>pass</type>
4904         <interface>wan</interface>
4905         <ipprotocol>inet</ipprotocol>
4906         <tag/>
4907         <tagged/>
4908         <max/>
4909         <max-src-nodes/>
4910         <max-src-conn/>
4911         <max-src-states/>
4912         <statetimeout/>
4913         <statetype>keep state</statetype>
4914         <os/>
4915         <protocol>tcp/udp</protocol>
4916         <source>
4917             <any/>
4918         </source>
4919         <destination>
4920             <network>lan</network>
4921             <port>53</port>
4922         </destination>
4923         <descr><![CDATA[Allow DNS traffic to LAN nodes]]></descr>
4924         <updated>

```

```

4925         <time>1493313314</time>
4926         <username>admin@10.97.67.143</username>
4927     </updated>
4928     <created>
4929         <time>1493313314</time>
4930         <username>admin@10.97.67.143</username>
4931     </created>
4932 </rule>
4933 <rule>
4934     <id/>
4935     <tracker>1493312231</tracker>
4936     <type>pass</type>
4937     <interface>wan</interface>
4938     <ipprotocol>inet</ipprotocol>
4939     <tag/>
4940     <tagged/>
4941     <max/>
4942     <max-src-nodes/>
4943     <max-src-conn/>
4944     <max-src-states/>
4945     <statetimeout/>
4946     <statetype>keep state</statetype>
4947     <os/>
4948     <protocol>tcp</protocol>
4949     <source>
4950         <any/>
4951     </source>
4952     <destination>
4953         <network>lan</network>
4954         <port>636</port>
4955     </destination>
4956     <descr><![CDATA[Allow LDAPs traffic to LAN nodes]]></descr>
4957     <updated>
4958         <time>1493312231</time>
4959         <username>admin@10.97.67.143</username>
4960     </updated>
4961     <created>
4962         <time>1493312231</time>
4963         <username>admin@10.97.67.143</username>
4964     </created>

```

```

4965         </rule>
4966     <rule>
4967         <id/>
4968         <tracker>1493311864</tracker>
4969         <type>pass</type>
4970         <interface>wan</interface>
4971         <ipprotocol>inet</ipprotocol>
4972         <tag/>
4973         <tagged/>
4974         <max/>
4975         <max-src-nodes/>
4976         <max-src-conn/>
4977         <max-src-states/>
4978         <statetimeout/>
4979         <statetype>keep state</statetype>
4980         <os/>
4981         <protocol>tcp</protocol>
4982         <source>
4983             <any/>
4984         </source>
4985         <destination>
4986             <network>lan</network>
4987             <port>22</port>
4988         </destination>
4989         <descr><![CDATA[Allow SSH traffic to LAN nodes ]]></descr>
4990         <updated>
4991             <time>1493311864</time>
4992             <username>admin@10.97.67.143</username>
4993         </updated>
4994         <created>
4995             <time>1493311864</time>
4996             <username>admin@10.97.67.143</username>
4997         </created>
4998     </rule>
4999     <rule>
5000         <id/>
5001         <tracker>1493311502</tracker>
5002         <type>pass</type>
5003         <interface>wan</interface>
5004         <ipprotocol>inet</ipprotocol>

```

```

5005         <tag/>
5006         <tagged/>
5007         <max/>
5008         <max-src-nodes/>
5009         <max-src-conn/>
5010         <max-src-states/>
5011         <statetimeout/>
5012         <statetype>keep state</statetype>
5013         <os/>
5014         <protocol>tcp/udp</protocol>
5015         <source>
5016             <network>lan</network>
5017         </source>
5018         <destination>
5019             <any/>
5020         </destination>
5021         <descr><![CDATA[Allow all LAN traffic to go to anywhere --Applied
5022 to]]></descr>
5023         <updated>
5024             <time>1493311502</time>
5025             <username>admin@10.97.67.143</username>
5026         </updated>
5027         <created>
5028             <time>1493311502</time>
5029             <username>admin@10.97.67.143</username>
5030         </created>
5031     </rule>
5032     <rule>
5033         <id/>
5034         <tracker>1493311408</tracker>
5035         <type>pass</type>
5036         <interface>wan</interface>
5037         <ipprotocol>inet</ipprotocol>
5038         <tag/>
5039         <tagged/>
5040         <max/>
5041         <max-src-nodes/>
5042         <max-src-conn/>
5043         <max-src-states/>
5044         <statetimeout/>

```

```

5045         <statetype>keep state</statetype>
5046     </os>
5047     <protocol>tcp</protocol>
5048     <source>
5049         <any/>
5050     </source>
5051     <destination>
5052         <network>wanip</network>
5053         <port>80</port>
5054     </destination>
5055     <descr><![CDATA[Allow to Port 80 on Firewall WAN]]></descr>
5056     <updated>
5057         <time>1493311408</time>
5058         <username>admin@10.97.67.143</username>
5059     </updated>
5060     <created>
5061         <time>1493311408</time>
5062         <username>admin@10.97.67.143</username>
5063     </created>
5064 </rule>
5065 <rule>
5066     <id/>
5067     <tracker>1493312279</tracker>
5068     <type>pass</type>
5069     <interface>wan</interface>
5070     <ipprotocol>inet</ipprotocol>
5071     <tag/>
5072     <tagged/>
5073     <max/>
5074     <max-src-nodes/>
5075     <max-src-conn/>
5076     <max-src-states/>
5077     <statetimeout/>
5078     <statetype>keep state</statetype>
5079     <os/>
5080     <protocol>tcp</protocol>
5081     <source>
5082         <any/>
5083     </source>
5084     <destination>

```



```

5085         <network>wanip</network>
5086         <port>443</port>
5087     </destination>
5088     <descr><![CDATA[Allow to Port 443 on Firewall WAN]]></descr>
5089     <updated>
5090         <time>1493312279</time>
5091         <username>admin@10.97.67.143</username>
5092     </updated>
5093     <created>
5094         <time>1493312279</time>
5095         <username>admin@10.97.67.143</username>
5096     </created>
5097 </rule>
5098 <rule>
5099     <id/>
5100     <tracker>1493311302</tracker>
5101     <type>pass</type>
5102     <interface>wan</interface>
5103     <ipprotocol>inet</ipprotocol>
5104     <tag/>
5105     <tagged/>
5106     <max/>
5107     <max-src-nodes/>
5108     <max-src-conn/>
5109     <max-src-states/>
5110     <statetimeout/>
5111     <statetype>keep state</statetype>
5112     <os/>
5113     <protocol>tcp</protocol>
5114     <source>
5115         <any/>
5116     </source>
5117     <destination>
5118         <network>lan</network>
5119         <port>3389</port>
5120     </destination>
5121     <descr><![CDATA[Allow RDP to LAN nodes]]></descr>
5122     <updated>
5123         <time>1493311302</time>
5124         <username>admin@10.97.67.143</username>

```

```

5125         </updated>
5126         <created>
5127             <time>1493311302</time>
5128             <username>admin@10.97.67.143</username>
5129         </created>
5130     </rule>
5131     <rule>
5132         <id/>
5133         <tracker>1469127156</tracker>
5134         <type>pass</type>
5135         <interface>wan</interface>
5136         <ipprotocol>inet</ipprotocol>
5137         <tag/>
5138         <tagged/>
5139         <max/>
5140         <max-src-nodes/>
5141         <max-src-conn/>
5142         <max-src-states/>
5143         <statetimeout/>
5144         <statetype>keep state</statetype>
5145         <os/>
5146         <protocol>tcp/udp</protocol>
5147         <source>
5148             <any/>
5149         </source>
5150         <destination>
5151             <any/>
5152         </destination>
5153         <disabled/>
5154         <descr/>
5155         <created>
5156             <time>1469127156</time>
5157             <username>admin@192.168.13.132</username>
5158         </created>
5159         <updated>
5160             <time>1493311628</time>
5161             <username>admin@10.97.67.143</username>
5162         </updated>
5163     </rule>
5164     <rule>

```

```

5165         <id/>
5166         <tracker>1480964347</tracker>
5167         <type>pass</type>
5168         <interface>wan</interface>
5169         <ipprotocol>inet</ipprotocol>
5170         <tag/>
5171         <tagged/>
5172         <max/>
5173         <max-src-nodes/>
5174         <max-src-conn/>
5175         <max-src-states/>
5176         <statetimeout/>
5177         <statetype>keep state</statetype>
5178         <os/>
5179         <source>
5180             <address>192.168.14.111</address>
5181         </source>
5182         <destination>
5183             <any/>
5184         </destination>
5185         <disabled/>
5186         <descr><![CDATA[Allow Radiant (192.168.14.111) to Get Subnet 19
5187 with]]></descr>
5188         <created>
5189             <time>1480964347</time>
5190             <username>admin@10.97.67.144</username>
5191         </created>
5192         <updated>
5193             <time>1493311596</time>
5194             <username>admin@10.97.67.143</username>
5195         </updated>
5196     </rule>
5197     <rule>
5198         <id/>
5199         <tracker>1480964466</tracker>
5200         <type>pass</type>
5201         <interface>wan</interface>
5202         <ipprotocol>inet</ipprotocol>
5203         <tag/>
5204         <tagged/>

```

```

5205         <max/>
5206         <max-src-nodes/>
5207         <max-src-conn/>
5208         <max-src-states/>
5209         <statetimeout/>
5210         <statetype>keep state</statetype>
5211         <os/>
5212         <source>
5213             <address>192.168.17.100</address>
5214         </source>
5215         <destination>
5216             <any/>
5217         </destination>
5218         <disabled/>
5219         <descr><![CDATA[Allow Radiant (192.168.17.100) to Get Subnet 19
5220 from]]></descr>
5221         <created>
5222             <time>1480964466</time>
5223             <username>admin@10.97.67.144</username>
5224         </created>
5225         <updated>
5226             <time>1493311572</time>
5227             <username>admin@10.97.67.143</username>
5228         </updated>
5229     </rule>
5230     <rule>
5231         <id/>
5232         <tracker>1465935224</tracker>
5233         <type>pass</type>
5234         <interface>wan</interface>
5235         <ipprotocol>inet</ipprotocol>
5236         <tag/>
5237         <tagged/>
5238         <max/>
5239         <max-src-nodes/>
5240         <max-src-conn/>
5241         <max-src-states/>
5242         <statetimeout/>
5243         <statetype>keep state</statetype>
5244         <os/>

```

```

5245         <protocol>icmp</protocol>
5246         <source>
5247             <any/>
5248         </source>
5249         <destination>
5250             <any/>
5251         </destination>
5252         <descr/>
5253         <updated>
5254             <time>1465935224</time>
5255             <username>admin@192.168.18.100</username>
5256         </updated>
5257         <created>
5258             <time>1465935224</time>
5259             <username>admin@192.168.18.100</username>
5260         </created>
5261     </rule>
5262     <rule>
5263         <id/>
5264         <tracker>1469127171</tracker>
5265         <type>pass</type>
5266         <interface>lan</interface>
5267         <ipprotocol>inet</ipprotocol>
5268         <tag/>
5269         <tagged/>
5270         <max/>
5271         <max-src-nodes/>
5272         <max-src-conn/>
5273         <max-src-states/>
5274         <statetimeout/>
5275         <statetype>keep state</statetype>
5276         <os/>
5277         <protocol>tcp/udp</protocol>
5278         <source>
5279             <any/>
5280         </source>
5281         <destination>
5282             <any/>
5283         </destination>
5284         <disabled/>

```

```

5285         <descr/>
5286         <created>
5287             <time>1469127171</time>
5288             <username>admin@192.168.13.132</username>
5289         </created>
5290         <updated>
5291             <time>1493322054</time>
5292             <username>admin@10.97.67.143</username>
5293         </updated>
5294     </rule>
5295     <rule>
5296         <id/>
5297         <tracker>1465935241</tracker>
5298         <type>pass</type>
5299         <interface>lan</interface>
5300         <ipprotocol>inet</ipprotocol>
5301         <tag/>
5302         <tagged/>
5303         <max/>
5304         <max-src-nodes/>
5305         <max-src-conn/>
5306         <max-src-states/>
5307         <statetimeout/>
5308         <statetype>keep state</statetype>
5309         <os/>
5310         <protocol>icmp</protocol>
5311         <source>
5312             <any/>
5313         </source>
5314         <destination>
5315             <any/>
5316         </destination>
5317         <descr/>
5318         <updated>
5319             <time>1465935241</time>
5320             <username>admin@192.168.18.100</username>
5321         </updated>
5322         <created>
5323             <time>1465935241</time>
5324             <username>admin@192.168.18.100</username>

```

```

5325         </created>
5326     </rule>
5327     <rule>
5328         <type>pass</type>
5329         <ipprotocol>inet</ipprotocol>
5330         <descr><![CDATA[Default allow LAN to any rule]]></descr>
5331         <interface>lan</interface>
5332         <tracker>0100000101</tracker>
5333         <source>
5334             <network>lan</network>
5335         </source>
5336         <destination>
5337             <any/>
5338         </destination>
5339     </rule>
5340     <rule>
5341         <type>pass</type>
5342         <ipprotocol>inet6</ipprotocol>
5343         <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
5344         <interface>lan</interface>
5345         <tracker>0100000102</tracker>
5346         <source>
5347             <network>lan</network>
5348         </source>
5349         <destination>
5350             <any/>
5351         </destination>
5352     </rule>
5353     <separator>
5354         <wan/>
5355         <lan/>
5356         <floatingrules/>
5357     </separator>
5358     <bypassstaticroutes>yes</bypassstaticroutes>
5359 </filter>
5360 <shaper>
5361 </shaper>
5362 <ipsec/>
5363 <aliases/>
5364 <proxyarp/>

```

```

5365         <cron>
5366             <item>
5367                 <minute>1,31</minute>
5368                 <hour>0-5</hour>
5369                 <mday>*</mday>
5370                 <month>*</month>
5371                 <wday>*</wday>
5372                 <who>root</who>
5373                 <command>/usr/bin/nice -n20 adjkerntz -a</command>
5374             </item>
5375             <item>
5376                 <minute>1</minute>
5377                 <hour>3</hour>
5378                 <mday>1</mday>
5379                 <month>*</month>
5380                 <wday>*</wday>
5381                 <who>root</who>
5382                 <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
5383             </item>
5384             <item>
5385                 <minute>*/60</minute>
5386                 <hour>*</hour>
5387                 <mday>*</mday>
5388                 <month>*</month>
5389                 <wday>*</wday>
5390                 <who>root</who>
5391                 <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
5392 sshlockout</command>
5393             </item>
5394             <item>
5395                 <minute>*/60</minute>
5396                 <hour>*</hour>
5397                 <mday>*</mday>
5398                 <month>*</month>
5399                 <wday>*</wday>
5400                 <who>root</who>
5401                 <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
5402 webConfiguratorlockout</command>
5403             </item>
5404             <item>

```



```

5405         <minute>1</minute>
5406         <hour>1</hour>
5407         <mday>*</mday>
5408         <month>*</month>
5409         <wday>*</wday>
5410         <who>root</who>
5411         <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
5412     </item>
5413     <item>
5414         <minute>*/60</minute>
5415         <hour>*</hour>
5416         <mday>*</mday>
5417         <month>*</month>
5418         <wday>*</wday>
5419         <who>root</who>
5420         <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
5421 virusprot</command>
5422     </item>
5423     <item>
5424         <minute>30</minute>
5425         <hour>12</hour>
5426         <mday>*</mday>
5427         <month>*</month>
5428         <wday>*</wday>
5429         <who>root</who>
5430         <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
5431     </item>
5432 </cron>
5433 <wol/>
5434 <rrd>
5435     <enable/>
5436 </rrd>
5437 <load_balancer>
5438     <monitor_type>
5439         <name>ICMP</name>
5440         <type>icmp</type>
5441         <descr><![CDATA[ICMP]]></descr>
5442         <options/>
5443     </monitor_type>
5444     <monitor_type>

```

```

5445         <name>TCP</name>
5446         <type>tcp</type>
5447         <descr><![CDATA[Generic TCP]]></descr>
5448         <options/>
5449     </monitor_type>
5450     <monitor_type>
5451         <name>HTTP</name>
5452         <type>http</type>
5453         <descr><![CDATA[Generic HTTP]]></descr>
5454         <options>
5455             <path></path>
5456             <host/>
5457             <code>200</code>
5458         </options>
5459     </monitor_type>
5460     <monitor_type>
5461         <name>HTTPS</name>
5462         <type>https</type>
5463         <descr><![CDATA[Generic HTTPS]]></descr>
5464         <options>
5465             <path></path>
5466             <host/>
5467             <code>200</code>
5468         </options>
5469     </monitor_type>
5470     <monitor_type>
5471         <name>SMTP</name>
5472         <type>send</type>
5473         <descr><![CDATA[Generic SMTP]]></descr>
5474         <options>
5475             <send/>
5476             <expect>220 *</expect>
5477         </options>
5478     </monitor_type>
5479 </load_balancer>
5480 <widgets>
5481     <sequence>system_information:col1:open,gateways:col1:open,interfaces:col2:open<
5482 /sequence>
5483 </widgets>
5484 <openvpn/>

```

```

5486     <dnshaper>
5487     </dnshaper>
5488     <unbound>
5489         <enable/>
5490         <dnssec/>
5491         <active_interface/>
5492         <outgoing_interface/>
5493         <custom_options/>
5494         <hideidentity/>
5495         <hideversion/>
5496         <dnssecstripped/>
5497     </unbound>
5498     <dhcpdv6>
5499         <lan>
5500             <range>
5501                 <from>::1000</from>
5502                 <to>::2000</to>
5503             </range>
5504             <ramode>assist</ramode>
5505             <rapriority>medium</rapriority>
5506         </lan>
5507     </dhcpdv6>
5508     <cert>
5509         <refid>5720a0502b277</refid>
5510         <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
5511         <type>server</type>
5512         <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXXZ0F3SUJBZ0lCQURBTkNa3
5513 Foa2lHOXcwQkFRc0ZBREncdERFTElBa0dBMVVfQmhnNQ1ZWtXgKRGpBTUJnTlZCQWdUQ1ZOMFlYUmxNUkV3RHdZ
5514 RFZRUUhFd2hNYjJOaGJHbDB1VEU0TURZR0ExVUVDaE12Y0daVApVzV6WlNCM1pXSkrImjVtYVdkMWNtRjBiM0
5515 lnVTJWc1ppMVRhV2RlWldRZlEyVnlkR2xtYVdOaGRHVXhLREFTcKJna3Foa2lHOXcwQkNRRVdHV0ZrYlZsdVFI
5516 Qm1VMlZlYzJVdWJHOWpZV3hrYjIxaGFxNHhIakFjQmdOVkZBTUVQKRlhCbVUyVnVjMlV0TlRjeU1HRXdOVEF5WW
5517 pJM056QWVGdzB4TmBME1qY3hNVEU1TkRSYU1JRzBNUN3Q1FZRFZRUUdF
5518 d0pWVXpFT01Bd0dBMVVfQ0JNRlUzUmhkr1V4RVRBUEJnTlZCQWNUCkNFeHZZMkZzYVhSNU1UZ3d0Z11EVlFRS0
5519 V5OXDabE5sYm5ObElIZGxZa052YmlacFozVnlZWfJ2Y2lCVFpXeg0KTFZOCfoYNWxaQ0JEWlhKMGFxWnBZMkYw
5520 WlRfb01DWUdDU3FHU01m0RRRUpBU1laWVdSdGFxNUFjRlplUWlcllegpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
5521 dBMVVFQXhNVMNHw1RaVzV6WlMwMU56SXdzVEExTURKaU1qYzNNSU1CCklqQU5CZ2txaGtpRz13MEJBUEUUGQUFP
5522 Q0FROEFNSU1CQ2dLQ0FRRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
5523 hDODBHU0dhZnJENWdqTFRwZkNNMHlzbEFpVlZK1hDYjdNa2o0dmtTMgpmBz14emNyaDUrNVlaYlBHeXRla2ls
5524 ZWR4bjFweFl6S1l1ZXZkdnlKb1lRMCTnTks0dkFjYnRhTUfoZjh1ZkRfClhrc1NVQ0N5YTFrbEYxNWJGZmcyUG
5525 E0eGRvMk9PNUJ5RzBrV0NKU2o4K1RlWnVkJFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
5526 ZEFiUEhjWGC5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXdlSEZwd3J1LytYWExieEcrcD
5527 dwYXI0aHR0UFRDcm1lNmFqQVVTNmpvN05kOE1QNWpZl1kzR0h2Zjh1ZkRfClhrc1NVQ0N5YTFrbEYxNWJGZmcyUG
5528 V1IwVEJBSXdbREFSQmdsZ2hrZ0JodmhDQVFRUJBTUNCa0F3TXdxZS1lJWkkKQV1iNFFnRU5CQ1lXSkU5d1pXNV
5529 RVMHdnUjJWdVpYSmhkR1ZrSUZOBNuWmxjaUJEWlhKMGFxWnBZMkYwWlRBZApCZ05WSFE0RUZnUVU3K1lLRmNp
5530 OFFVSGhTZ0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCMlRDQjFvQVU3K1lLCkZjaThRVUhoU2dMRHY4RUNzY0
5531 NKd0FLaGdicWtnYmN3Z2JReEN6QUppCZ05WQkFZVEFsV1RNU3R3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
5532 VUVCElJVEc5a1lXeHBkSGt4TORBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWdWpRMj1lWm1sbmRYSmhkRz15SU
5533

```

```

5534 ZObGJHWRVMmxuYm1Wa0lFTmxjblJwWm1sallYUmXNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJrQnda
5535 bE5sYm5ObExteHZZMkZzWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
5536 56ZUNBUUF3SFFZRFZSMGxCQl13RkFZSut3WUJCUVVIQXdfR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd0lG
5537 b0RBTKJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZfPQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmTNaTB5M0
5538 9PWGtzWES1cEM2dTd6Ukl3WjEvRjYyRUp3ODlUOWx4Y01ZelZOTm5Idlg0bXFPRUCUWJhRU42NEKxOHFud3Zm
5539 S2JrREZvRThMR1hSdzBkMnAyTGVmYtd4YTIvSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG
5540 c4bGdrcVc3dStlb0lDNDJIBvJkOURCTm1zdfJ4RVlNMkFLQkFsZG1LYStvRUY1VUwwCm43aXpVn1Z4dHJWMTJv
5541 TTdyS1lRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VnFULldDZGo3dDdIVG9ob0RFYzEKSk1kOVpPSmR2QmZLVU
5542 1sUWlELElyswSpTa1FXRDczWkdsaEhTK2tOeWcladJhUjUwYj3hWm9zQnNjSUZDa0pFbgbp0UT09C10tLS0tRU5E
5543 IENFUlRJRklDQVRFLS0tLS0K</crt>
5544
5545 <prv>LS0tLS1CRUDJTIBQUklQVRFIETFWS0tLS0tCk1JSUV2Z0lCQURBTkJna3Foa2lHOXcwQkFRRU
5546 ZBQVNQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M0lhY1kKMjN3YkNKR1htWFJWky9odVVKeFdc3hxb3M4
5547 eGxiY3YyRUX6UVPjWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMwltqM0hOeXVibjdsaGxzOG
5548 JLMjZTS1Y1M0dmVlhGak1saXhXOG0vSW1oaERUNHcWdTl4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEPyV1NVWFhs
5549 c1YrRfk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcwdeKQVdEQkQzNDg5OHRUalhrOVNpblNaclREbn
5550 dKTmo3cHAWQnM4ZHh1RDBjL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
5551 dHZFYjZudWxxdmlHMjA5TUtlSzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUprRF
5552 pxU3duMnNTUTh0SVNBTVUvRW0zcXhzb3BzdZB4cWNScmF0Ed4VmQKejBpOU1KbkZVQWFletQvL3JldndhZWlP
5553 R3RYSmZ2ai9jSnY3cmJIWGIzYkYtVW9hcDhXy0RjdnVSMm1HRUZyWQpCL3hjNVpINTlaTUfabWE1VWVQLzNjcD
5554 lzNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQX4dSGJZWWhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1Zn1P
5555 UzAvbXlMNU5YLzVoRklPNmFDc0xlUjZ4N1Rza2FDQU9FYlViT29qUXkKc09XewphbEtTUWZ3WEdzdVM0bXdyR2
5556 hMZ0NRYlB2MnE5VONia0VMNEZUZmRzRlZXCjHBRNGlZVWtwNzhMY1FPMgppsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
5557 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUe0NzNMUWoxcExLsmRZN2JxCmtMU3NVt0ZhTUZlZG1xU2ttbzh3Qj
5558 lpMXhzbElLQUd0M3U4dtdMZlZtU2lybnMwVVBtMHRVUDRyQXmZvVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
5559 OGttbFJnUFRmVHVPaGnWmgVkamQwK1E5Y2VlY25kaFp3UEl6TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHhbm
5560 NBRDhVYThDZl1lFQXpzYjYzbzRBSh1YNjZkcEJ6TG1zYzZxS2d2ZG4xazhVcm02N3RuK2M3NkVhSEtZTlK0RjdH
5561 S0dFSklYeU0yQTJTelAzdm03Rmk4eGRtblgrSX4d5cUx5t1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUpOK0I3Sm
5562 Z2RjYrK2tHa1NHOGxaN0VLY2lUc1kzRVJxOURsSk94Nk1ROFEwMDNsTHvtQQpJZmlDWlpRSUQ1OENnWUJjamFO
5563 dk5obnFJOG9rWghBUjR2c3NtNgpWb0tYU1ZScjRiVHo5MDfWOGdReXNCWkt0CnlUS2V6VThuUVZvtjNYWmVMbC
5564 8rVEcwYVpKOTZHKy9nNTRWZmZqWTRlelVSChhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
5565 QWY5Mi9CbHZJR25FS1pMdnhLWtdVMXl1Ib1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
5566 VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
5567 RG1hZGsvKy9Ud2UvVk1KbmX2TW9zs3VjTG42Y1c2eGVhR1hFc3FoUj1hbkWzRjMKcEpUSGg4Y3FNTdqdkRRN0
5568 FBamdYQmxrb3pOVnNMZThiWWpkcHRlMVBRS0JnQ0xDR0RlRXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1Rlczdu
5569 WjRoM3ZRODI1ZkQxbGVzVjBYdJlcvJqeFEvSDgxMHRGdlp3C9uSVdycnRCZlZlClUzStHhYnpnUUtWoeWzZj
5570 VadTAxY1pZVks5TU0FIUFRHYm5jb1IzbGVpYjNleUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
5571 OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>
5572
5573 </cert>
5574
5575 <revision>
5576
5577 <time>1493327306</time>
5578
5579 <description><![CDATA[admin@10.97.67.143: /firewall_rules_edit.php made
5580 unknown change]]></description>
5581
5582 <username>admin@10.97.67.143</username>
5583
5584 </revision>
5585
5586 <gateways>
5587
5588 <gateway_item>
5589
5590 <interface>wan</interface>
5591
5592 <gateway>192.168.13.1</gateway>
5593
5594 <name>GW_WAN_2</name>
5595
5596 <weight>1</weight>
5597
5598 <ipprotocol>inet</ipprotocol>
5599
5600 <interval/>
5601
5602 <descr><![CDATA[Interface wan Gateway]]></descr>

```

```

5588         </gateway_item>
5589         <gateway_item>
5590             <interface>wan</interface>
5591             <gateway>192.168.13.17</gateway>
5592             <name>GW_VLAN17</name>
5593             <weight>1</weight>
5594             <ipprotocol>inet</ipprotocol>
5595             <descr><![CDATA[Gateway to VLAN 17]]></descr>
5596         </gateway_item>
5597     </gateways>
5598     <ppps/>
5599     <dyndnses/>
5600 </pfSense>
5601 2.10.3 Firewall Configuration for ID-ARM Subnet
5602 <?xml version="1.0"?>
5603 <pfSense>
5604     <version>15.4</version>
5605     <lastchange/>
5606     <theme>pfSense_ng</theme>
5607     <system>
5608         <optimization>normal</optimization>
5609         <hostname>FS-ARM</hostname>
5610         <domain>FS-ARM.gov</domain>
5611         <group>
5612             <name>all</name>
5613             <description><![CDATA[All Users]]></description>
5614             <scope>system</scope>
5615             <gid>1998</gid>
5616             <member>0</member>
5617         </group>
5618         <group>
5619             <name>admins</name>
5620             <description><![CDATA[System Administrators]]></description>
5621             <scope>system</scope>
5622             <gid>1999</gid>
5623             <member>0</member>
5624             <priv>page-all</priv>
5625         </group>
5626         <user>

```

```

5627         <name>admin</name>
5628         <descr><![CDATA[System Administrator]]></descr>
5629         <scope>system</scope>
5630         <groupname>admins</groupname>
5631         <password>$1$dSJmFph$GvZ7.1UbuWu.Yb8etC0re.</password>
5632         <uid>0</uid>
5633         <priv>user-shell-access</priv>
5634     </user>
5635     <nextuid>2000</nextuid>
5636     <nextgid>2000</nextgid>
5637     <timezone>America/New_York</timezone>
5638     <time-update-interval/>
5639     <timeservers>10.97.74.8</timeservers>
5640     <webgui>
5641         <protocol>http</protocol>
5642         <loginautocomplete/>
5643         <ssl-certref>5720a0502b277</ssl-certref>
5644         <dashboardcolumns>2</dashboardcolumns>
5645         <port/>
5646         <max_procs>2</max_procs>
5647         <nohttppreferercheck/>
5648     </webgui>
5649     <disablenatreflection>yes</disablenatreflection>
5650     <disablesegmentationoffloading/>
5651     <disablelargereceiveoffloading/>
5652     <ipv6allow/>
5653     <powerd_ac_mode>hadp</powerd_ac_mode>
5654     <powerd_battery_mode>hadp</powerd_battery_mode>
5655     <powerd_normal_mode>hadp</powerd_normal_mode>
5656     <bogons>
5657         <interval>monthly</interval>
5658     </bogons>
5659     <language>en_US</language>
5660     <dns1gw>GW_WAN</dns1gw>
5661     <dns2gw>GW_WAN</dns2gw>
5662     <dns3gw>none</dns3gw>
5663     <dns4gw>none</dns4gw>
5664     <dnsserver>10.97.74.8</dnsserver>
5665     <dnsserver>10.63.255.2</dnsserver>
5666     <serialspeed>115200</serialspeed>

```

```

5667         <primaryconsole>serial</primaryconsole>
5668     </system>
5669     <interfaces>
5670         <wan>
5671             <if>em0</if>
5672             <descr><![CDATA[WAN]]></descr>
5673             <enable/>
5674             <spoofmac/>
5675             <ipaddr>192.168.13.14</ipaddr>
5676             <subnet>24</subnet>
5677             <gateway>GW_WAN</gateway>
5678         </wan>
5679         <lan>
5680             <enable/>
5681             <if>em1</if>
5682             <ipaddr>192.168.14.1</ipaddr>
5683             <subnet>24</subnet>
5684             <ipaddrv6/>
5685             <subnetv6/>
5686             <media/>
5687             <mediaopt/>
5688             <track6-interface>wan</track6-interface>
5689             <track6-prefix-id>0</track6-prefix-id>
5690             <gateway/>
5691             <gatewayv6/>
5692         </lan>
5693     </interfaces>
5694     <staticroutes>
5695         <route>
5696             <network>192.168.17.0/24</network>
5697             <gateway>GW_VLAN17</gateway>
5698             <descr><![CDATA[Route to VLAN 2017]]></descr>
5699         </route>
5700         <route>
5701             <network>192.168.16.0/24</network>
5702             <gateway>GW_VLAN16</gateway>
5703             <descr><![CDATA[Route to VLAN 2016]]></descr>
5704         </route>
5705         <route>
5706             <network>192.168.15.0/24</network>

```

```

5707         <gateway>GW_VLAN15</gateway>
5708         <descr><![CDATA[Route to VLAN 2015]]></descr>
5709     </route>
5710     <route>
5711         <network>192.168.18.0/24</network>
5712         <gateway>GW_VLAN18</gateway>
5713         <descr><![CDATA[Route to VLAN 2018]]></descr>
5714     </route>
5715     <route>
5716         <network>192.168.19.0/24</network>
5717         <gateway>GW_VLAN19</gateway>
5718         <descr><![CDATA[Route to VLAN 2019]]></descr>
5719     </route>
5720 </staticroutes>
5721 <dhcpd>
5722     <lan>
5723         <enable/>
5724         <range>
5725             <from>192.168.14.100</from>
5726             <to>192.168.14.150</to>
5727         </range>
5728     </lan>
5729     <opt1>
5730         <enable/>
5731         <range>
5732             <from>192.168.14.100</from>
5733             <to>192.168.14.150</to>
5734         </range>
5735     </opt1>
5736     <opt2>
5737         <enable/>
5738         <range>
5739             <from>192.168.15.100</from>
5740             <to>192.168.15.150</to>
5741         </range>
5742     </opt2>
5743     <opt3>
5744         <enable/>
5745         <range>
5746             <from>192.168.16.100</from>

```



```

5747             <to>192.168.16.150</to>
5748         </range>
5749     </opt3>
5750 </dhcpd>
5751 <snmpd>
5752     <syslocation/>
5753     <syscontact/>
5754     <rocommunity>public</rocommunity>
5755 </snmpd>
5756 <diag>
5757     <ipv6nat>
5758         <ipaddr/>
5759     </ipv6nat>
5760 </diag>
5761 <bridge/>
5762 <syslog/>
5763 <nat>
5764     <outbound>
5765         <mode>disabled</mode>
5766     </outbound>
5767 </nat>
5768 <filter>
5769     <rule>
5770         <id/>
5771         <tracker>1481037990</tracker>
5772         <type>pass</type>
5773         <interface>wan</interface>
5774         <ipprotocol>inet</ipprotocol>
5775         <tag/>
5776         <tagged/>
5777         <direction>any</direction>
5778         <quick>yes</quick>
5779         <floating>yes</floating>
5780         <max/>
5781         <max-src-nodes/>
5782         <max-src-conn/>
5783         <max-src-states/>
5784         <statetimeout/>
5785         <statetype>keep state</statetype>
5786     </rule>

```

```

5787         <protocol>tcp/udp</protocol>
5788         <source>
5789             <any/>
5790         </source>
5791         <destination>
5792             <network>lan</network>
5793             <port>3389</port>
5794         </destination>
5795         <descr><![CDATA[Allow RDP to LAN nodes]]></descr>
5796         <created>
5797             <time>1481037990</time>
5798             <username>admin@10.97.67.155</username>
5799         </created>
5800         <updated>
5801             <time>1493324042</time>
5802             <username>admin@10.97.67.143</username>
5803         </updated>
5804     </rule>
5805     <rule>
5806         <id/>
5807         <tracker>1481038086</tracker>
5808         <type>pass</type>
5809         <interface>wan</interface>
5810         <ipprotocol>inet</ipprotocol>
5811         <tag/>
5812         <tagged/>
5813         <direction>any</direction>
5814         <quick>yes</quick>
5815         <floating>yes</floating>
5816         <max/>
5817         <max-src-nodes/>
5818         <max-src-conn/>
5819         <max-src-states/>
5820         <statetimeout/>
5821         <statetype>keep state</statetype>
5822         <os/>
5823         <protocol>tcp/udp</protocol>
5824         <source>
5825             <any/>
5826         </source>

```

```

5827         <destination>
5828             <network>lan</network>
5829             <port>2389</port>
5830         </destination>
5831         <descr><![CDATA[Allow Connection to Radiant Port 2389]]></descr>
5832         <created>
5833             <time>1481038086</time>
5834             <username>admin@10.97.67.155</username>
5835         </created>
5836         <updated>
5837             <time>1493324258</time>
5838             <username>admin@10.97.67.143</username>
5839         </updated>
5840     </rule>
5841     <rule>
5842         <id/>
5843         <tracker>1493650861</tracker>
5844         <type>pass</type>
5845         <interface>wan</interface>
5846         <ipprotocol>inet</ipprotocol>
5847         <tag/>
5848         <tagged/>
5849         <direction>any</direction>
5850         <quick>yes</quick>
5851         <floating>yes</floating>
5852         <max/>
5853         <max-src-nodes/>
5854         <max-src-conn/>
5855         <max-src-states/>
5856         <statetimeout/>
5857         <statetype>keep state</statetype>
5858         <os/>
5859         <protocol>tcp/udp</protocol>
5860         <source>
5861             <any/>
5862         </source>
5863         <destination>
5864             <network>lan</network>
5865             <port>389</port>
5866         </destination>

```

```

5867         <descr><![CDATA[Allow Connection to Port 389 in LAN]]></descr>
5868         <updated>
5869             <time>1493650861</time>
5870             <username>admin@10.97.67.135</username>
5871         </updated>
5872         <created>
5873             <time>1493650861</time>
5874             <username>admin@10.97.67.135</username>
5875         </created>
5876     </rule>
5877     <rule>
5878         <id/>
5879         <tracker>1493650905</tracker>
5880         <type>pass</type>
5881         <interface>wan</interface>
5882         <ipprotocol>inet</ipprotocol>
5883         <tag/>
5884         <tagged/>
5885         <direction>any</direction>
5886         <quick>yes</quick>
5887         <floating>yes</floating>
5888         <max/>
5889         <max-src-nodes/>
5890         <max-src-conn/>
5891         <max-src-states/>
5892         <statetimeout/>
5893         <statetype>keep state</statetype>
5894         <os></os>
5895         <protocol>tcp/udp</protocol>
5896         <source>
5897             <any/>
5898         </source>
5899         <destination>
5900             <network>lan</network>
5901             <port>636</port>
5902         </destination>
5903         <descr><![CDATA[Allow Connection to Port 636 in LAN]]></descr>
5904         <updated>
5905             <time>1493650905</time>
5906             <username>admin@10.97.67.135</username>

```

```

5907         </updated>
5908         <created>
5909             <time>1493650905</time>
5910             <username>admin@10.97.67.135</username>
5911         </created>
5912     </rule>
5913     <rule>
5914         <id/>
5915         <tracker>1493328157</tracker>
5916         <type>pass</type>
5917         <interface>wan</interface>
5918         <ipprotocol>inet</ipprotocol>
5919         <tag/>
5920         <tagged/>
5921         <direction>any</direction>
5922         <quick>yes</quick>
5923         <floating>yes</floating>
5924         <max/>
5925         <max-src-nodes/>
5926         <max-src-conn/>
5927         <max-src-states/>
5928         <statetimeout/>
5929         <statetype>keep state</statetype>
5930         <os/>
5931         <protocol>tcp/udp</protocol>
5932         <source>
5933             <any/>
5934         </source>
5935         <destination>
5936             <network>lan</network>
5937             <port>8089</port>
5938         </destination>
5939         <descr><![CDATA[Allow Connection to Radiant Port 8089]]></descr>
5940         <updated>
5941             <time>1493328157</time>
5942             <username>admin@10.97.67.143</username>
5943         </updated>
5944         <created>
5945             <time>1493328157</time>
5946             <username>admin@10.97.67.143</username>

```

```

5947         </created>
5948     </rule>
5949     <rule>
5950         <id/>
5951         <tracker>1493328202</tracker>
5952         <type>pass</type>
5953         <interface>wan</interface>
5954         <ipprotocol>inet</ipprotocol>
5955         <tag/>
5956         <tagged/>
5957         <direction>any</direction>
5958         <quick>yes</quick>
5959         <floating>yes</floating>
5960         <max/>
5961         <max-src-nodes/>
5962         <max-src-conn/>
5963         <max-src-states/>
5964         <statetimeout/>
5965         <statetype>keep state</statetype>
5966         <os/>
5967         <protocol>tcp/udp</protocol>
5968         <source>
5969             <any/>
5970         </source>
5971         <destination>
5972             <network>lan</network>
5973             <port>8090</port>
5974         </destination>
5975         <descr><![CDATA[Allow Connection to Radiant Port 8090]]></descr>
5976         <updated>
5977             <time>1493328202</time>
5978             <username>admin@10.97.67.143</username>
5979         </updated>
5980         <created>
5981             <time>1493328202</time>
5982             <username>admin@10.97.67.143</username>
5983         </created>
5984     </rule>
5985     <rule>
5986         <id/>

```

```

5987         <tracker>1493327695</tracker>
5988         <type>pass</type>
5989         <interface>wan</interface>
5990         <ipprotocol>inet</ipprotocol>
5991         <tag/>
5992         <tagged/>
5993         <direction>any</direction>
5994         <quick>yes</quick>
5995         <floating>yes</floating>
5996         <max/>
5997         <max-src-nodes/>
5998         <max-src-conn/>
5999         <max-src-states/>
6000         <statetimeout/>
6001         <statetype>keep state</statetype>
6002         <os/>
6003         <protocol>tcp/udp</protocol>
6004         <source>
6005             <any/>
6006         </source>
6007         <destination>
6008             <network>lan</network>
6009             <port>8443</port>
6010         </destination>
6011         <descr><![CDATA[Allow Connection to Nextlabs port 8443]]></descr>
6012         <updated>
6013             <time>1493327695</time>
6014             <username>admin@10.97.67.143</username>
6015         </updated>
6016         <created>
6017             <time>1493327695</time>
6018             <username>admin@10.97.67.143</username>
6019         </created>
6020     </rule>
6021     <rule>
6022         <id/>
6023         <tracker>1493327739</tracker>
6024         <type>pass</type>
6025         <interface>wan</interface>
6026         <ipprotocol>inet</ipprotocol>

```

```

6027         <tag/>
6028         <tagged/>
6029         <direction>any</direction>
6030         <quick>yes</quick>
6031         <floating>yes</floating>
6032         <max/>
6033         <max-src-nodes/>
6034         <max-src-conn/>
6035         <max-src-states/>
6036         <statetimeout/>
6037         <statetype>keep state</statetype>
6038         <os/>
6039         <protocol>tcp</protocol>
6040         <source>
6041             <any/>
6042         </source>
6043         <destination>
6044             <network>lan</network>
6045             <port>443</port>
6046         </destination>
6047         <descr><![CDATA[Allow Connection to Nextlabs port 443]]></descr>
6048         <updated>
6049             <time>1493327739</time>
6050             <username>admin@10.97.67.143</username>
6051         </updated>
6052         <created>
6053             <time>1493327739</time>
6054             <username>admin@10.97.67.143</username>
6055         </created>
6056     </rule>
6057     <rule>
6058         <id/>
6059         <tracker>1493327782</tracker>
6060         <type>pass</type>
6061         <interface>wan</interface>
6062         <ipprotocol>inet</ipprotocol>
6063         <tag/>
6064         <tagged/>
6065         <direction>any</direction>
6066         <quick>yes</quick>

```



```

6067         <floating>yes</floating>
6068         <max/>
6069         <max-src-nodes/>
6070         <max-src-conn/>
6071         <max-src-states/>
6072         <statetimeout/>
6073         <statetype>keep state</statetype>
6074         <os/>
6075         <protocol>tcp/udp</protocol>
6076         <source>
6077             <any/>
6078         </source>
6079         <destination>
6080             <any/>
6081             <port>9233</port>
6082         </destination>
6083         <descr><![CDATA[Allow Connection to Nextlabs port 9233]]></descr>
6084         <created>
6085             <time>1493327782</time>
6086             <username>admin@10.97.67.143</username>
6087         </created>
6088         <updated>
6089             <time>1493327896</time>
6090             <username>admin@10.97.67.143</username>
6091         </updated>
6092     </rule>
6093     <rule>
6094         <id/>
6095         <tracker>1493327859</tracker>
6096         <type>pass</type>
6097         <interface>wan</interface>
6098         <ipprotocol>inet</ipprotocol>
6099         <tag/>
6100         <tagged/>
6101         <direction>any</direction>
6102         <quick>yes</quick>
6103         <floating>yes</floating>
6104         <max/>
6105         <max-src-nodes/>
6106         <max-src-conn/>

```

```

6107         <max-src-states/>
6108         <statetimeout/>
6109         <statetype>keep state</statetype>
6110         <os/>
6111         <protocol>tcp/udp</protocol>
6112         <source>
6113             <any/>
6114         </source>
6115         <destination>
6116             <any/>
6117             <port>19888</port>
6118         </destination>
6119         <descr><![CDATA[Allow Connection to Nextlabs port 19888]]></descr>
6120         <updated>
6121             <time>1493327859</time>
6122             <username>admin@10.97.67.143</username>
6123         </updated>
6124         <created>
6125             <time>1493327859</time>
6126             <username>admin@10.97.67.143</username>
6127         </created>
6128     </rule>
6129 <rule>
6130     <id/>
6131     <tracker>1493325919</tracker>
6132     <type>pass</type>
6133     <interface>wan</interface>
6134     <ipprotocol>inet</ipprotocol>
6135     <tag/>
6136     <tagged/>
6137     <direction>any</direction>
6138     <quick>yes</quick>
6139     <floating>yes</floating>
6140     <max/>
6141     <max-src-nodes/>
6142     <max-src-conn/>
6143     <max-src-states/>
6144     <statetimeout/>
6145     <statetype>keep state</statetype>
6146     <os/>

```

```

6147         <protocol>tcp/udp</protocol>
6148         <source>
6149             <network>lan</network>
6150         </source>
6151         <destination>
6152             <any/>
6153             <port>53</port>
6154         </destination>
6155         <descr><![CDATA[Allow DNS port 53 going out]]></descr>
6156         <created>
6157             <time>1493325919</time>
6158             <username>admin@10.97.67.143</username>
6159         </created>
6160         <updated>
6161             <time>1493326213</time>
6162             <username>admin@10.97.67.143</username>
6163         </updated>
6164     </rule>
6165     <rule>
6166         <id/>
6167         <tracker>1493328002</tracker>
6168         <type>pass</type>
6169         <ipprotocol>inet</ipprotocol>
6170         <tag/>
6171         <tagged/>
6172         <direction>any</direction>
6173         <quick>yes</quick>
6174         <floating>yes</floating>
6175         <max/>
6176         <max-src-nodes/>
6177         <max-src-conn/>
6178         <max-src-states/>
6179         <statetimeout/>
6180         <statetype>keep state</statetype>
6181         <os/>
6182         <protocol>tcp/udp</protocol>
6183         <source>
6184             <any/>
6185         </source>
6186         <destination>

```

```

6187             <any/>
6188             <port>2000</port>
6189         </destination>
6190         <descr><![CDATA[Allow Connection to Nextlabs port 2000]]></descr>
6191         <updated>
6192             <time>1493328002</time>
6193             <username>admin@10.97.67.143</username>
6194         </updated>
6195         <created>
6196             <time>1493328002</time>
6197             <username>admin@10.97.67.143</username>
6198         </created>
6199     </rule>
6200     <rule>
6201         <id/>
6202         <tracker>1481037313</tracker>
6203         <type>pass</type>
6204         <interface>wan</interface>
6205         <ipprotocol>inet</ipprotocol>
6206         <tag/>
6207         <tagged/>
6208         <max/>
6209         <max-src-nodes/>
6210         <max-src-conn/>
6211         <max-src-states/>
6212         <statetimeout/>
6213         <statetype>keep state</statetype>
6214         <os/>
6215         <source>
6216             <address>192.168.14.111</address>
6217         </source>
6218         <destination>
6219             <any/>
6220         </destination>
6221         <descr><![CDATA[Allow Radiant (192.168.14.111) to get out with any
6222 p]]></descr>
6223         <created>
6224             <time>1481037313</time>
6225             <username>admin@10.97.67.155</username>
6226         </created>

```

```

6227         <updated>
6228             <time>1481037359</time>
6229             <username>admin@10.97.67.155</username>
6230         </updated>
6231         <disabled/>
6232     </rule>
6233     <rule>
6234         <id/>
6235         <tracker>1480537443</tracker>
6236         <type>pass</type>
6237         <interface>wan</interface>
6238         <ipprotocol>inet</ipprotocol>
6239         <tag/>
6240         <tagged/>
6241         <max/>
6242         <max-src-nodes/>
6243         <max-src-conn/>
6244         <max-src-states/>
6245         <statetimeout/>
6246         <statetype>keep state</statetype>
6247         <os/>
6248         <source>
6249             <any/>
6250         </source>
6251         <destination>
6252             <any/>
6253         </destination>
6254         <descr><![CDATA[Allow Everything]]></descr>
6255         <updated>
6256             <time>1480537443</time>
6257             <username>admin@192.168.13.139</username>
6258         </updated>
6259         <created>
6260             <time>1480537443</time>
6261             <username>admin@192.168.13.139</username>
6262         </created>
6263         <disabled/>
6264     </rule>
6265     <rule>
6266         <id/>

```

```

6267         <tracker>1466105351</tracker>
6268         <type>pass</type>
6269         <interface>wan</interface>
6270         <ipprotocol>inet</ipprotocol>
6271         <tag/>
6272         <tagged/>
6273         <max/>
6274         <max-src-nodes/>
6275         <max-src-conn/>
6276         <max-src-states/>
6277         <statetimeout/>
6278         <statetype>keep state</statetype>
6279         <os/>
6280         <protocol>udp</protocol>
6281         <source>
6282             <any/>
6283         </source>
6284         <destination>
6285             <any/>
6286         </destination>
6287         <descr/>
6288         <updated>
6289             <time>1466105351</time>
6290             <username>admin@192.168.13.101</username>
6291         </updated>
6292         <created>
6293             <time>1466105351</time>
6294             <username>admin@192.168.13.101</username>
6295         </created>
6296         <disabled/>
6297     </rule>
6298     <rule>
6299         <id/>
6300         <tracker>1465934980</tracker>
6301         <type>pass</type>
6302         <interface>wan</interface>
6303         <ipprotocol>inet</ipprotocol>
6304         <tag/>
6305         <tagged/>
6306         <max/>

```

```

6307         <max-src-nodes/>
6308         <max-src-conn/>
6309         <max-src-states/>
6310         <statetimeout/>
6311         <statetype>keep state</statetype>
6312         <os/>
6313         <protocol>icmp</protocol>
6314         <source>
6315             <any/>
6316         </source>
6317         <destination>
6318             <any/>
6319         </destination>
6320         <descr/>
6321         <updated>
6322             <time>1465934980</time>
6323             <username>admin@192.168.14.100</username>
6324         </updated>
6325         <created>
6326             <time>1465934980</time>
6327             <username>admin@192.168.14.100</username>
6328         </created>
6329     </rule>
6330 <rule>
6331     <id/>
6332     <tracker>1461788221</tracker>
6333     <type>pass</type>
6334     <interface>wan</interface>
6335     <ipprotocol>inet</ipprotocol>
6336     <tag/>
6337     <tagged/>
6338     <max/>
6339     <max-src-nodes/>
6340     <max-src-conn/>
6341     <max-src-states/>
6342     <statetimeout/>
6343     <statetype>keep state</statetype>
6344     <os/>
6345     <protocol>tcp</protocol>
6346     <source>

```

```

6347         <any/>
6348     </source>
6349     <destination>
6350         <network>wanip</network>
6351         <port>80</port>
6352     </destination>
6353     <descr><![CDATA[Allow to Port 80 on Firewall WAN]]></descr>
6354     <created>
6355         <time>1461788221</time>
6356         <username>admin@192.168.1.2</username>
6357     </created>
6358     <updated>
6359         <time>1493323649</time>
6360         <username>admin@10.97.67.143</username>
6361     </updated>
6362 </rule>
6363 <rule>
6364     <type>pass</type>
6365     <interface>wan</interface>
6366     <ipprotocol>inet</ipprotocol>
6367     <descr><![CDATA[Easy Rule: Passed from Firewall Log
6368 View]]></descr>
6369     <protocol>udp</protocol>
6370     <source>
6371         <address>192.168.13.101</address>
6372     </source>
6373     <destination>
6374         <address>192.168.13.102</address>
6375         <port>137</port>
6376     </destination>
6377     <created>
6378         <time>1466105470</time>
6379         <username>Easy Rule</username>
6380     </created>
6381 </rule>
6382 <rule>
6383     <id/>
6384     <tracker>1480537570</tracker>
6385     <type>pass</type>
6386     <interface>lan</interface>

```



```

6387         <ipprotocol>inet</ipprotocol>
6388     </tag>
6389 </tagged/>
6390 </max/>
6391 </max-src-nodes/>
6392 </max-src-conn/>
6393 </max-src-states/>
6394 </statetimeout/>
6395 <statetype>keep state</statetype>
6396 </os/>
6397 <source>
6398     <any/>
6399 </source>
6400 <destination>
6401     <any/>
6402 </destination>
6403 <descr><![CDATA[All Everything from LAN Interface]]></descr>
6404 <updated>
6405     <time>1480537570</time>
6406     <username>admin@192.168.13.139</username>
6407 </updated>
6408 <created>
6409     <time>1480537570</time>
6410     <username>admin@192.168.13.139</username>
6411 </created>
6412 </disabled/>
6413 </rule>
6414 <rule>
6415     <id/>
6416     <tracker>1466105363</tracker>
6417     <type>pass</type>
6418     <interface>lan</interface>
6419     <ipprotocol>inet</ipprotocol>
6420 </tag>
6421 </tagged/>
6422 </max/>
6423 </max-src-nodes/>
6424 </max-src-conn/>
6425 </max-src-states/>
6426 </statetimeout/>

```

```

6427         <statetype>keep state</statetype>
6428     </os>
6429     <protocol>udp</protocol>
6430     <source>
6431         <any/>
6432     </source>
6433     <destination>
6434         <any/>
6435     </destination>
6436     <descr/>
6437     <updated>
6438         <time>1466105363</time>
6439         <username>admin@192.168.13.101</username>
6440     </updated>
6441     <created>
6442         <time>1466105363</time>
6443         <username>admin@192.168.13.101</username>
6444     </created>
6445     <disabled/>
6446 </rule>
6447 <rule>
6448     <id/>
6449     <tracker>1465934995</tracker>
6450     <type>pass</type>
6451     <interface>lan</interface>
6452     <ipprotocol>inet</ipprotocol>
6453     <tag/>
6454     <tagged/>
6455     <max/>
6456     <max-src-nodes/>
6457     <max-src-conn/>
6458     <max-src-states/>
6459     <statetimeout/>
6460     <statetype>keep state</statetype>
6461     <os/>
6462     <protocol>icmp</protocol>
6463     <source>
6464         <any/>
6465     </source>
6466     <destination>

```

```

6467             <any/>
6468         </destination>
6469         <descr/>
6470         <updated>
6471             <time>1465934995</time>
6472             <username>admin@192.168.14.100</username>
6473         </updated>
6474         <created>
6475             <time>1465934995</time>
6476             <username>admin@192.168.14.100</username>
6477         </created>
6478     </rule>
6479     <rule>
6480         <id/>
6481         <tracker>1465915373</tracker>
6482         <type>pass</type>
6483         <interface>lan</interface>
6484         <ipprotocol>inet</ipprotocol>
6485         <tag/>
6486         <tagged/>
6487         <max/>
6488         <max-src-nodes/>
6489         <max-src-conn/>
6490         <max-src-states/>
6491         <statetimeout/>
6492         <statetype>keep state</statetype>
6493         <os/>
6494         <protocol>tcp</protocol>
6495         <source>
6496             <any/>
6497         </source>
6498         <destination>
6499             <any/>
6500         </destination>
6501         <descr><![CDATA[Allow Any Any]]></descr>
6502         <updated>
6503             <time>1465915373</time>
6504             <username>admin@192.168.14.100</username>
6505         </updated>
6506         <created>

```

```

6507             <time>1465915373</time>
6508             <username>admin@192.168.14.100</username>
6509         </created>
6510         <disabled/>
6511     </rule>
6512     <rule>
6513         <type>pass</type>
6514         <ipprotocol>inet</ipprotocol>
6515         <descr><![CDATA[Default allow LAN to any rule]]></descr>
6516         <interface>lan</interface>
6517         <tracker>0100000101</tracker>
6518         <source>
6519             <network>lan</network>
6520         </source>
6521         <destination>
6522             <any/>
6523         </destination>
6524     </rule>
6525     <rule>
6526         <type>pass</type>
6527         <ipprotocol>inet6</ipprotocol>
6528         <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
6529         <interface>lan</interface>
6530         <tracker>0100000102</tracker>
6531         <source>
6532             <network>lan</network>
6533         </source>
6534         <destination>
6535             <any/>
6536         </destination>
6537     </rule>
6538     <separator>
6539         <wan/>
6540         <lan/>
6541         <floatingrules/>
6542     </separator>
6543 </filter>
6544 <shaper>
6545 </shaper>
6546 <ipsec/>

```

## DRAFT

```
6547     <aliases/>
6548     <proxyarp/>
6549     <cron>
6550         <item>
6551             <minute>1,31</minute>
6552             <hour>0-5</hour>
6553             <mday>*</mday>
6554             <month>*</month>
6555             <wday>*</wday>
6556             <who>root</who>
6557             <command>/usr/bin/nice -n20 adjkerntz -a</command>
6558         </item>
6559         <item>
6560             <minute>1</minute>
6561             <hour>3</hour>
6562             <mday>1</mday>
6563             <month>*</month>
6564             <wday>*</wday>
6565             <who>root</who>
6566             <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
6567         </item>
6568         <item>
6569             <minute>*/60</minute>
6570             <hour>*</hour>
6571             <mday>*</mday>
6572             <month>*</month>
6573             <wday>*</wday>
6574             <who>root</who>
6575             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
6576 sshlockout</command>
6577         </item>
6578         <item>
6579             <minute>*/60</minute>
6580             <hour>*</hour>
6581             <mday>*</mday>
6582             <month>*</month>
6583             <wday>*</wday>
6584             <who>root</who>
6585             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
6586 webConfiguratorlockout</command>
```

```

6587         </item>
6588     <item>
6589         <minute>1</minute>
6590         <hour>1</hour>
6591         <mday>*</mday>
6592         <month>*</month>
6593         <wday>*</wday>
6594         <who>root</who>
6595         <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
6596     </item>
6597     <item>
6598         <minute>*/60</minute>
6599         <hour>*</hour>
6600         <mday>*</mday>
6601         <month>*</month>
6602         <wday>*</wday>
6603         <who>root</who>
6604         <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
6605 virusprot</command>
6606     </item>
6607     <item>
6608         <minute>30</minute>
6609         <hour>12</hour>
6610         <mday>*</mday>
6611         <month>*</month>
6612         <wday>*</wday>
6613         <who>root</who>
6614         <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
6615     </item>
6616 </cron>
6617 <wol/>
6618 <rrd>
6619     <enable/>
6620 </rrd>
6621 <load_balancer>
6622     <monitor_type>
6623         <name>ICMP</name>
6624         <type>icmp</type>
6625         <descr><![CDATA[ICMP]]></descr>
6626     <options/>

```

```

6627         </monitor_type>
6628     <monitor_type>
6629         <name>TCP</name>
6630         <type>tcp</type>
6631         <descr><![CDATA[Generic TCP]]></descr>
6632         <options/>
6633     </monitor_type>
6634     <monitor_type>
6635         <name>HTTP</name>
6636         <type>http</type>
6637         <descr><![CDATA[Generic HTTP]]></descr>
6638         <options>
6639             <path></path>
6640             <host/>
6641             <code>200</code>
6642         </options>
6643     </monitor_type>
6644     <monitor_type>
6645         <name>HTTPS</name>
6646         <type>https</type>
6647         <descr><![CDATA[Generic HTTPS]]></descr>
6648         <options>
6649             <path></path>
6650             <host/>
6651             <code>200</code>
6652         </options>
6653     </monitor_type>
6654     <monitor_type>
6655         <name>SMTP</name>
6656         <type>send</type>
6657         <descr><![CDATA[Generic SMTP]]></descr>
6658         <options>
6659             <send/>
6660             <expect>220 *</expect>
6661         </options>
6662     </monitor_type>
6663 </load_balancer>
6664 <widgets>
6665     <sequence>system_information:coll:open,gateways:coll:open,interfaces:col2:open<
6666 /sequence>

```

```

6668         </widgets>
6669         <openvpn/>
6670         <dnshaper>
6671         </dnshaper>
6672         <unbound>
6673             <enable/>
6674             <dnssec/>
6675             <active_interface/>
6676             <outgoing_interface/>
6677             <custom_options/>
6678             <hideidentity/>
6679             <hideversion/>
6680             <dnssecstripped/>
6681         </unbound>
6682         <dhcpdv6>
6683             <lan>
6684                 <range>
6685                     <from>::1000</from>
6686                     <to>::2000</to>
6687                 </range>
6688                 <ramode>assist</ramode>
6689                 <rapriority>medium</rapriority>
6690             </lan>
6691         </dhcpdv6>
6692         <cert>
6693             <refid>5720a0502b277</refid>
6694             <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
6695             <type>server</type>
6696             <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURSB0tLS0tCk1JSUZiVENkZXZ0F3SUJBZ0lCQURBTkNa3
6697             Foa2lHOXcwQkFRc0ZBREncdERFTE1Ba0dBmVVFQmhnQ1ZWTXgKRGPBTUJnTlZCQWdUQ1ZOMFlYUmXNUkV3RHdZ
6698             RFZRUUhFd2hnyjJOAGJHbDBlVEU0TURZROExVUVDaE12Y0daVApVzV6WlNCM1pXSkrImjVtYVdkMWNtrjBiM0
6699             lnVTJWclppMVRhV2RlWldRZ1EyVnlkR2xtYVdOaGRHVXhLREftCkNa3Foa2lHOXcwQkNRRVdHV0ZrYldsdVFI
6700             Qm1VM1ZlYzJVdWJHOWpZV3hrYjIxaGFxNHhIakFjQmdOVk1JBTBQK1hCbVUyVnVjM1V0TlRjeU1HRXdoVEF5WW
6701             pJM056QWVGdzB4TmBME1qY3hNVEU1TkRSYU1TlZCQWdUQ1ZOMFlYUmXNUkV3RHdZRFZRUUhFd2hnyjJOAGJHbDBlVEU0TURZROExVUVDaE12Y0daVApVzV6WlNCM1pXSkrImjVtYVdkMWNtrjBiM0
6702             d0pWVXpFT01Bd0dBmVVFQ0JNR1UzUmhkr1V4RVRBUEJnTlZCQWdUQ1ZOMFlYUmXNUkV3RHdZRFZRUUhFd2hnyjJOAGJHbDBlVEU0TURZROExVUVDaE12Y0daVApVzV6WlNCM1pXSkrImjVtYVdkMWNtrjBiM0
6703             V5OXDabE5sYm50bE1IZGxZa052Ym1acFozVnlZWFFJ2Y2lCVFpXeg0KTFZ0cFoyNWxaQ0JEWlhmGFxWnBZMkYw
6704             WlRfb01DWUdDU3FHU01m0RRRUpBU1laWVdSdGFxNUFjR1pUW1cllegpaUzVzYjJOAGJHbDBlVEU0TURZROExVUVDaE12Y0daVApVzV6WlNCM1pXSkrImjVtYVdkMWNtrjBiM0
6705             dBMVVFQXhNvMhWlRaVzV6WlMwMU56SXdxVEExTURKaU1qYzNNSU1CCKlqQU5CZ2tXaGtpRz13MEJBUBUUVGQUPP
6706             Q0FROEFNSU1CQ2dLQ0FRUF0L085aDlnt2R5R20yTnQ4R3dpUmw1bDAKVMZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
6707             hDODBHU0dhZnJENWdqctRWZkNNMh1zbEFPaV1ZK1hdyjdNa2o0dmtTMgpmBzl4emNyaDUrNV1aY1BHeXR1a2ls
6708             ZWR4bjFwFwF16S1l1zYXZkdnlKb1lRMctNTkx0dkFjYnRhTUfoZjh1ZkRfClhrc1NVQ0N5YTFrbEYxNWJGZmcyUG
6709             E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkcUFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
6710             ZEFiUEhJWgc5SFA0NFQybfNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXdlSEZwd3J1LytYWExieEcrcD
6711             dwYXI0aHR0UFRDcm1lNmFqQVVTNmpvN05kOE1QNWpzZ1kzR0h2Zjh1ZkRfClhrc1NVQ0N5YTFrbEYxNWJGZmcyUG
6712             V1IwVEJBBSXdbREFSQmdsZ2hrZ0JodmhDQVFRUJBTUNCa0F3TXdZS1lJWkkKQVliNFFnRU5CQ1lXSku5d1pXNV
6713             RVMHdnUjJWdVpYShmhR1ZrSUZ0bGNuWmxjaUJEWlhmGFxWnBZMkYwWlRbZApCZ05WSFE0RUZnUUVU3K1lLRmNp
6714

```



```

6715 OFFVSGhTZ0xEdjhFQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCM1RDQjFvQVU3K11LLCkZjaThRVUhoU2dMRHY4RUNzY0
6716 NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
6717 VUVCeE1JVEc5a1lXeHBkSGt4T0RBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaQpRMj1lWm1sbmRYSmhkRz15SU
6718 ZObGJHWXRVMmxuYm1Wa0lFTmxjblJwWm1sal1YUmXNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxcGJRQnda
6719 bE5sYm5ObExteHZZMkZzWkc5dFlXbHVNujR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRfV3TW1JeU
6720 56ZUNBUUF3SFFZRFZSMGxCQ113RkFZSut3WUJCUVVIQXdfR0NDc0dBuVVGQ0FJQwpNQXNHQTFVZER3UUVBd01G
6721 b0RBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZfPQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmtNaTB5M0
6722 9PWGtzWEs1cEM2dTd6Ukl3WjEvRjYyRUUp3ODlUOWx4Y01ZelZOTm5Idlg0bXFPRUCUWJhRU42NEkxOHFud3Zm
6723 S2JrREZvRThMRlhSdzBkMnAyTGVmYtD4YTIvSGNHc0xHTktPbkjxb3N4ejUrQ1B3ZwpWeVraTS9wV3p3aDdQRG
6724 c4bGdrcVc3dStlb01DNDJIBVJkOURCTmlzdfJ4RVlNMkFLQkFsZG1LYStvRUy1VUwwCm43aXpvN1Z4dHJWMTJv
6725 TTdyS1lRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VVnFULldDZGo3dDdIVG9ob0RFYzEKSklkOVpPsmR2QmZLVU
6726 1sUW1ELyswSVpTa1FXRDczWkdsEhTK2tOeWcladJhUjUwYj3Wm9zQnNjSUZDa0pFbgbp0UT09ci0tLS0tRU5E
6727 IENFULRJRklDQVRFLS0tLS0K</crt>
6728
6729 <prv>LS0tLS1CRUdJTiBQUklWQVRFIEtFWS0tLS0tCk1JSUV2Z01CQURBTkJna3Foa2lHOXcwQkFRRU
6730 ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M0lhY1kKMjN3YkNKR1htWFJWky9odVVKefDsc3hxb3M4
6731 eGxiY3UyRUx6UVPjWnArc1BtQ09yaWw4SXPuU3lVQTZKaG0lYwpKdnN5U1BpK1JMWitqM0hOeXV1bjdsaGxzOG
6732 JLMjZTS1Y1M0dmVlhGak1saXhOG0vSW1oaERUNHcWdTl4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEpyV1NVWFhs
6733 c1YrRFk5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcwdeKQVdEQkQzNDg5OHRUalhrOVNpb1NaclREbn
6734 dKTmo3cHAWQnM4ZHh1RDBjL2poUGFWSWNKem1vbKpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
6735 dHZFYjZudWxxdmlHMjA5TUtlSzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUppRRF
6736 pxU3duMnNTUTh0SVNBTVUvRUw0zcXhrb3BzdZB4cWNScmF0Ed4VmQKejBpOU1KbkZVQWFletQvL3JldndhZWlP
6737 R3RYSmZ2ai9jSnY3pzMJIWGIzYkYtVW9hcDhxY0RjdnVSMm1HRUZyWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjcD
6738 lzNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXh4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1Zn1P
6739 UzAvbXlmNU5YLzVoRklPNmFDc0x1UjZ4N1RZa2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
6740 hMZ0NRY1B2MnE5V0Nia0VMNEZUZmRzRlZXcHBRNGlZVWtwNzhMY1FPMgpsSGR5cTJxTmJsNDIwa3h5M2FnZlF2
6741 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUEN0NzNMUWoxcExLSmRZN2JxCMtMU3NVTOzhTUZlZG1xU2ttbzh3Qj
6742 lpMXhzbElLQud0M3U4dTdMz1ZtU2lybnMwVVBtMHRVUDRYQXMXzVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
6743 OGttbFJnUFRmVHVpAGNwMGVkamQwK1E5Y2V1Y25kaFp3UE16TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZNHhbm
6744 NBRDhVYThDZl1lFQXpYjYzbzRBSHlYNjZkcEJ6TG1zYzZxS2d2ZG4xazhVCM02N3RuK2M3NkVhSEtZT1k0RjdH
6745 S0dFSklYeU0yQTJTelAzdm03Rmk4eGRtblgrSXh4SGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1Zn1P
6746 Z2RjYrK2tHa1NHOGxaN0VLY2lUc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZm1DWlpRSUQ1OENnWUJjamFO
6747 dk5obnFJOG9rWGHBUjR2c3NtNGpWb0tYU1ZScjRIVHo5MDFwOGdReXNCWkt0CnlUS2V6VThuUVZvTjNYWmVMbC
6748 8rVEcwYVpKOTZHKy9nNTRWZmZgWTRlelVSChhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
6749 QWY5Mi9CbHZJR25FS1pMdnhLWtdVMXl1Ib1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
6750 VudmNUUjZxTzR0ekZtdG5TYWN3W1Ftb2UvdUVIaGE0bU84WTBcETNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
6751 RG1hZGsvKy9Ud2UvVklKbmX2TW9fS3VjTG42Y1c2eGVhR1hfC3FoUj1hbkWzRjMKcEpUSGg4Y3FsnTdqdkRRN0
6752 FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBR50JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1RlcZdu
6753 WjRoM3ZRODI1ZkQxbGVzVjBYdDl1cVJqeFEvSDgxMHRGdlp3cC9uSVdycnRCZlZLC1UzStHhYnpnUUtWOWEwrZj
6754 VadTAxY1pZV5k5TU0FIUFRHYm5jb1IzbGVpYjNLEUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
6755 OVFOVGJkQWJrCi0tLS0tRU5EIEFBSSVZBVEUgS0VZLS0tLS0K</prv>
6756
6757 </cert>
6758
6759 <revision>
6760
6761 <time>1493650905</time>
6762
6763 <description><![CDATA[admin@10.97.67.135: /firewall_rules_edit.php made
6764 unknown change]]></description>
6765
6766 <username>admin@10.97.67.135</username>
6767
6768 </revision>
6769
6770 <gateways>
6771
6772 <gateway_item>
6773
6774 <interface>lan</interface>
6775
6776 <gateway>dynamic</gateway>
6777
6778 <name>WAN_DHCP</name>
6779
6780 <weight>1</weight>
6781
6782 <ipprotocol>inet</ipprotocol>

```

```

6770         <descr><![CDATA[Interface WAN_DHCP Gateway]]></descr>
6771     </gateway_item>
6772     <gateway_item>
6773         <interface>lan</interface>
6774         <gateway>dynamic</gateway>
6775         <name>WAN_DHCP</name>
6776         <weight>1</weight>
6777         <ipprotocol>inet</ipprotocol>
6778         <descr><![CDATA[Interface WAN_DHCP Gateway]]></descr>
6779     </gateway_item>
6780     <gateway_item>
6781         <interface>lan</interface>
6782         <gateway>dynamic</gateway>
6783         <name>WAN_DHCP6</name>
6784         <weight>1</weight>
6785         <ipprotocol>inet6</ipprotocol>
6786         <descr><![CDATA[Interface WAN_DHCP6 Gateway]]></descr>
6787         <defaultgw/>
6788     </gateway_item>
6789     <gateway_item>
6790         <interface>wan</interface>
6791         <gateway>192.168.13.1</gateway>
6792         <name>GW_WAN</name>
6793         <weight>1</weight>
6794         <ipprotocol>inet</ipprotocol>
6795         <interval/>
6796         <descr><![CDATA[Interface wan Gateway]]></descr>
6797         <defaultgw/>
6798     </gateway_item>
6799     <gateway_item>
6800         <interface>wan</interface>
6801         <gateway>192.168.13.17</gateway>
6802         <name>GW_VLAN17</name>
6803         <weight>1</weight>
6804         <ipprotocol>inet</ipprotocol>
6805         <descr><![CDATA[Gateway to VLAN 17]]></descr>
6806     </gateway_item>
6807     <gateway_item>
6808         <interface>wan</interface>
6809         <gateway>192.168.13.16</gateway>

```

```

6810         <name>GW_VLAN16</name>
6811         <weight>1</weight>
6812         <ipprotocol>inet</ipprotocol>
6813         <descr><![CDATA[Gateway to VLAN 16]]></descr>
6814     </gateway_item>
6815     <gateway_item>
6816         <interface>wan</interface>
6817         <gateway>192.168.13.15</gateway>
6818         <name>GW_VLAN15</name>
6819         <weight>1</weight>
6820         <ipprotocol>inet</ipprotocol>
6821         <descr><![CDATA[Gateway to VLAN 15]]></descr>
6822     </gateway_item>
6823     <gateway_item>
6824         <interface>wan</interface>
6825         <gateway>192.168.13.18</gateway>
6826         <name>GW_VLAN18</name>
6827         <weight>1</weight>
6828         <ipprotocol>inet</ipprotocol>
6829         <descr><![CDATA[Gateway to VLAN 18]]></descr>
6830     </gateway_item>
6831     <gateway_item>
6832         <interface>wan</interface>
6833         <gateway>192.168.13.19</gateway>
6834         <name>GW_VLAN19</name>
6835         <weight>1</weight>
6836         <ipprotocol>inet</ipprotocol>
6837         <descr><![CDATA[Gateway to VLAN 19]]></descr>
6838     </gateway_item>
6839 </gateways>
6840 <ppps/>
6841 <dyndnses/>
6842 </pfSense>
6843 2.10.4 Firewall Configuration for Private Cloud Subnet
6844 <?xml version="1.0"?>
6845 <pfSense>
6846     <version>15.4</version>
6847     <lastchange/>
6848     <theme>pfSense_ng</theme>

```

```

6849     <system>
6850         <optimization>normal</optimization>
6851         <hostname>FS-ARM</hostname>
6852         <domain>FS-ARM.gov</domain>
6853         <group>
6854             <name>all</name>
6855             <description><![CDATA[All Users]]></description>
6856             <scope>system</scope>
6857             <gid>1998</gid>
6858             <member>0</member>
6859         </group>
6860         <group>
6861             <name>admins</name>
6862             <description><![CDATA[System Administrators]]></description>
6863             <scope>system</scope>
6864             <gid>1999</gid>
6865             <member>0</member>
6866             <priv>page-all</priv>
6867         </group>
6868         <user>
6869             <name>admin</name>
6870             <descr><![CDATA[System Administrator]]></descr>
6871             <scope>system</scope>
6872             <groupname>admins</groupname>
6873             <password>$1$dSJmFph$GvZ7.1UbuWu.Yb8etC0re.</password>
6874             <uid>0</uid>
6875             <priv>user-shell-access</priv>
6876         </user>
6877         <nextuid>2000</nextuid>
6878         <nextgid>2000</nextgid>
6879         <timezone>America/New_York</timezone>
6880         <time-update-interval/>
6881         <timeservers>10.97.74.8</timeservers>
6882         <webgui>
6883             <protocol>http</protocol>
6884             <loginautocomplete/>
6885             <ssl-certref>5720a0502b277</ssl-certref>
6886             <dashboardcolumns>2</dashboardcolumns>
6887             <port/>
6888             <max_procs>2</max_procs>

```

```

6889         <nohttppreferercheck/>
6890     </webgui>
6891     <disablesegmentationoffloading/>
6892     <disablelargereceiveoffloading/>
6893     <ipv6allow/>
6894     <powerd_ac_mode>hadp</powerd_ac_mode>
6895     <powerd_battery_mode>hadp</powerd_battery_mode>
6896     <powerd_normal_mode>hadp</powerd_normal_mode>
6897     <bogons>
6898         <interval>monthly</interval>
6899     </bogons>
6900     <language>en_US</language>
6901     <dns1gw>GW_WAN</dns1gw>
6902     <dns2gw>GW_WAN</dns2gw>
6903     <dns3gw>none</dns3gw>
6904     <dns4gw>none</dns4gw>
6905     <dnsserver>10.97.74.8</dnsserver>
6906     <dnsserver>10.63.255.2</dnsserver>
6907     <maximumstates/>
6908     <aliasesresolveinterval/>
6909     <maximumtableentries/>
6910     <maximumfrags/>
6911     <enablenatreflectionpurenat>yes</enablenatreflectionpurenat>
6912     <enablebinatreflection>yes</enablebinatreflection>
6913     <enablenatreflectionhelper>yes</enablenatreflectionhelper>
6914     <reflectiontimeout/>
6915     <serialspeed>115200</serialspeed>
6916     <primaryconsole>serial</primaryconsole>
6917 </system>
6918 <interfaces>
6919     <wan>
6920         <if>em0</if>
6921         <descr><![CDATA[WAN]]></descr>
6922         <enable/>
6923         <spoofmac/>
6924         <ipaddr>192.168.13.20</ipaddr>
6925         <subnet>24</subnet>
6926         <gateway>GW_WAN_2</gateway>
6927         <ipaddrv6/>
6928         <subnetv6/>

```

```

6929             <gatewayv6/>
6930         </wan>
6931     <lan>
6932         <enable/>
6933         <if>em1</if>
6934         <ipaddr>192.168.20.1</ipaddr>
6935         <subnet>24</subnet>
6936         <ipaddrv6/>
6937         <subnetv6/>
6938         <media/>
6939         <mediaopt/>
6940         <track6-interface>wan</track6-interface>
6941         <track6-prefix-id>0</track6-prefix-id>
6942         <gateway/>
6943         <gatewayv6/>
6944     </lan>
6945 </interfaces>
6946 <staticroutes/>
6947 <dhcpd>
6948     <lan>
6949         <enable/>
6950         <range>
6951             <from>192.168.20.100</from>
6952             <to>192.168.20.150</to>
6953         </range>
6954     </lan>
6955     <opt1>
6956         <enable/>
6957         <range>
6958             <from>192.168.14.100</from>
6959             <to>192.168.14.150</to>
6960         </range>
6961     </opt1>
6962     <opt2>
6963         <enable/>
6964         <range>
6965             <from>192.168.15.100</from>
6966             <to>192.168.15.150</to>
6967         </range>
6968     </opt2>

```

```

6969         <opt3>
6970             <enable/>
6971             <range>
6972                 <from>192.168.16.100</from>
6973                 <to>192.168.16.150</to>
6974             </range>
6975         </opt3>
6976     </dhcpcd>
6977     <snmpd>
6978         <syslocation/>
6979         <syscontact/>
6980         <rocommunity>public</rocommunity>
6981     </snmpd>
6982     <diag>
6983         <ipv6nat>
6984             <ipaddr/>
6985         </ipv6nat>
6986     </diag>
6987     <bridge/>
6988     <syslog/>
6989     <nat>
6990         <outbound>
6991             <mode>automatic</mode>
6992         </outbound>
6993     </nat>
6994     <filter>
6995         <rule>
6996             <id/>
6997             <tracker>1493654453</tracker>
6998             <type>pass</type>
6999             <interface>wan</interface>
7000             <ipprotocol>inet</ipprotocol>
7001             <tag/>
7002             <tagged/>
7003             <direction>any</direction>
7004             <quick>yes</quick>
7005             <floating>yes</floating>
7006             <max/>
7007             <max-src-nodes/>
7008             <max-src-conn/>

```

```

7009         <max-src-states/>
7010         <statetimeout/>
7011         <statetype>keep state</statetype>
7012         <os/>
7013         <protocol>tcp</protocol>
7014         <source>
7015             <any/>
7016         </source>
7017         <destination>
7018             <network>lan</network>
7019             <port>443</port>
7020         </destination>
7021         <descr><![CDATA[Allow HTTPS connection to LAN server]]></descr>
7022         <updated>
7023             <time>1493654453</time>
7024             <username>admin@10.97.67.135</username>
7025         </updated>
7026         <created>
7027             <time>1493654453</time>
7028             <username>admin@10.97.67.135</username>
7029         </created>
7030     </rule>
7031     <rule>
7032         <id/>
7033         <tracker>1493654529</tracker>
7034         <type>pass</type>
7035         <interface>wan</interface>
7036         <ipprotocol>inet</ipprotocol>
7037         <tag/>
7038         <tagged/>
7039         <direction>any</direction>
7040         <quick>yes</quick>
7041         <floating>yes</floating>
7042         <max/>
7043         <max-src-nodes/>
7044         <max-src-conn/>
7045         <max-src-states/>
7046         <statetimeout/>
7047         <statetype>keep state</statetype>
7048         <os/>

```



```

7049         <protocol>tcp</protocol>
7050     <source>
7051         <any/>
7052     </source>
7053     <destination>
7054         <network>lan</network>
7055         <port>80</port>
7056     </destination>
7057     <descr><![CDATA[Allow HTTP connection to LAN server]]></descr>
7058     <updated>
7059         <time>1493654529</time>
7060         <username>admin@10.97.67.135</username>
7061     </updated>
7062     <created>
7063         <time>1493654529</time>
7064         <username>admin@10.97.67.135</username>
7065     </created>
7066 </rule>
7067 <rule>
7068     <id/>
7069     <tracker>1493654337</tracker>
7070     <type>pass</type>
7071     <interface>wan</interface>
7072     <ipprotocol>inet</ipprotocol>
7073     <tag/>
7074     <tagged/>
7075     <direction>any</direction>
7076     <quick>yes</quick>
7077     <floating>yes</floating>
7078     <max/>
7079     <max-src-nodes/>
7080     <max-src-conn/>
7081     <max-src-states/>
7082     <statetimeout/>
7083     <statetype>keep state</statetype>
7084     <os/>
7085     <protocol>tcp</protocol>
7086     <source>
7087         <any/>
7088     </source>

```

```

7089         <destination>
7090             <network>lan</network>
7091             <port>3389</port>
7092         </destination>
7093         <descr><![CDATA[Allow RDP Connection to LAN servers]]></descr>
7094         <created>
7095             <time>1493654337</time>
7096             <username>admin@10.97.67.135</username>
7097         </created>
7098         <updated>
7099             <time>1493654474</time>
7100             <username>admin@10.97.67.135</username>
7101         </updated>
7102     </rule>
7103     <rule>
7104         <id/>
7105         <tracker>1469131237</tracker>
7106         <type>pass</type>
7107         <interface>wan</interface>
7108         <ipprotocol>inet</ipprotocol>
7109         <tag/>
7110         <tagged/>
7111         <max/>
7112         <max-src-nodes/>
7113         <max-src-conn/>
7114         <max-src-states/>
7115         <statetimeout/>
7116         <statetype>keep state</statetype>
7117         <os/>
7118         <protocol>tcp</protocol>
7119         <source>
7120             <any/>
7121         </source>
7122         <destination>
7123             <network>wanip</network>
7124             <port>80</port>
7125         </destination>
7126         <descr><![CDATA[Allow Port 80 on WAN ]]></descr>
7127         <created>
7128             <time>1469131237</time>

```

```

7129             <username>admin@192.168.20.103</username>
7130         </created>
7131     <updated>
7132         <time>1493654100</time>
7133         <username>admin@10.97.67.135</username>
7134     </updated>
7135 </rule>
7136 <rule>
7137     <id/>
7138     <tracker>1465935224</tracker>
7139     <type>pass</type>
7140     <interface>wan</interface>
7141     <ipprotocol>inet</ipprotocol>
7142     <tag/>
7143     <tagged/>
7144     <max/>
7145     <max-src-nodes/>
7146     <max-src-conn/>
7147     <max-src-states/>
7148     <statetimeout/>
7149     <statetype>keep state</statetype>
7150     <os/>
7151     <protocol>icmp</protocol>
7152     <source>
7153         <any/>
7154     </source>
7155     <destination>
7156         <any/>
7157     </destination>
7158     <descr/>
7159     <updated>
7160         <time>1465935224</time>
7161         <username>admin@192.168.18.100</username>
7162     </updated>
7163     <created>
7164         <time>1465935224</time>
7165         <username>admin@192.168.18.100</username>
7166     </created>
7167 </rule>
7168 <rule>

```

```

7169         <id/>
7170         <tracker>1461788221</tracker>
7171         <type>pass</type>
7172         <interface>wan</interface>
7173         <ipprotocol>inet</ipprotocol>
7174         <tag/>
7175         <tagged/>
7176         <max/>
7177         <max-src-nodes/>
7178         <max-src-conn/>
7179         <max-src-states/>
7180         <statetimeout/>
7181         <statetype>keep state</statetype>
7182         <os/>
7183         <protocol>tcp</protocol>
7184         <source>
7185             <any/>
7186         </source>
7187         <destination>
7188             <network>wanip</network>
7189             <port>443</port>
7190         </destination>
7191         <descr><![CDATA[Allow Port 443 on WAN]]></descr>
7192         <created>
7193             <time>1461788221</time>
7194             <username>admin@192.168.1.2</username>
7195         </created>
7196         <updated>
7197             <time>1493654159</time>
7198             <username>admin@10.97.67.135</username>
7199         </updated>
7200     </rule>
7201     <rule>
7202         <id/>
7203         <tracker>1468437174</tracker>
7204         <type>pass</type>
7205         <interface>lan</interface>
7206         <ipprotocol>inet</ipprotocol>
7207         <tag/>
7208         <tagged/>

```

```

7209         <max/>
7210         <max-src-nodes/>
7211         <max-src-conn/>
7212         <max-src-states/>
7213         <statetimeout/>
7214         <statetype>keep state</statetype>
7215         <os/>
7216         <protocol>tcp/udp</protocol>
7217         <source>
7218             <any/>
7219         </source>
7220         <destination>
7221             <any/>
7222         </destination>
7223         <descr/>
7224         <updated>
7225             <time>1468437174</time>
7226             <username>admin@192.168.20.100</username>
7227         </updated>
7228         <created>
7229             <time>1468437174</time>
7230             <username>admin@192.168.20.100</username>
7231         </created>
7232         <disabled/>
7233     </rule>
7234 <rule>
7235     <id/>
7236     <tracker>1465935241</tracker>
7237     <type>pass</type>
7238     <interface>lan</interface>
7239     <ipprotocol>inet</ipprotocol>
7240     <tag/>
7241     <tagged/>
7242     <max/>
7243     <max-src-nodes/>
7244     <max-src-conn/>
7245     <max-src-states/>
7246     <statetimeout/>
7247     <statetype>keep state</statetype>
7248     <os/>

```

```

7249         <protocol>icmp</protocol>
7250         <source>
7251             <any/>
7252         </source>
7253         <destination>
7254             <any/>
7255         </destination>
7256         <descr/>
7257         <updated>
7258             <time>1465935241</time>
7259             <username>admin@192.168.18.100</username>
7260         </updated>
7261         <created>
7262             <time>1465935241</time>
7263             <username>admin@192.168.18.100</username>
7264         </created>
7265     </rule>
7266     <rule>
7267         <type>pass</type>
7268         <ipprotocol>inet</ipprotocol>
7269         <descr><![CDATA[Default allow LAN to any rule]]></descr>
7270         <interface>lan</interface>
7271         <tracker>0100000101</tracker>
7272         <source>
7273             <network>lan</network>
7274         </source>
7275         <destination>
7276             <any/>
7277         </destination>
7278     </rule>
7279     <rule>
7280         <type>pass</type>
7281         <ipprotocol>inet6</ipprotocol>
7282         <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
7283         <interface>lan</interface>
7284         <tracker>0100000102</tracker>
7285         <source>
7286             <network>lan</network>
7287         </source>
7288         <destination>

```

```

7289             <any/>
7290         </destination>
7291     </rule>
7292     <separator>
7293         <wan/>
7294         <lan/>
7295         <floatingrules/>
7296     </separator>
7297 </filter>
7298 <shaper>
7299 </shaper>
7300 <ipsec/>
7301 <aliases/>
7302 <proxyarp/>
7303 <cron>
7304     <item>
7305         <minute>1,31</minute>
7306         <hour>0-5</hour>
7307         <mday>*</mday>
7308         <month>*</month>
7309         <wday>*</wday>
7310         <who>root</who>
7311         <command>/usr/bin/nice -n20 adjkerntz -a</command>
7312     </item>
7313     <item>
7314         <minute>1</minute>
7315         <hour>3</hour>
7316         <mday>1</mday>
7317         <month>*</month>
7318         <wday>*</wday>
7319         <who>root</who>
7320         <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
7321     </item>
7322     <item>
7323         <minute>*/60</minute>
7324         <hour>*</hour>
7325         <mday>*</mday>
7326         <month>*</month>
7327         <wday>*</wday>
7328         <who>root</who>

```

```

7329             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
7330 sshlockout</command>
7331         </item>
7332         <item>
7333             <minute>*/60</minute>
7334             <hour>*</hour>
7335             <mday>*</mday>
7336             <month>*</month>
7337             <wday>*</wday>
7338             <who>root</who>
7339             <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
7340 webConfiguratorlockout</command>
7341     </item>
7342     <item>
7343         <minute>1</minute>
7344         <hour>1</hour>
7345         <mday>*</mday>
7346         <month>*</month>
7347         <wday>*</wday>
7348         <who>root</who>
7349         <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
7350     </item>
7351     <item>
7352         <minute>*/60</minute>
7353         <hour>*</hour>
7354         <mday>*</mday>
7355         <month>*</month>
7356         <wday>*</wday>
7357         <who>root</who>
7358         <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
7359 virusprot</command>
7360 </item>
7361 <item>
7362     <minute>30</minute>
7363     <hour>12</hour>
7364     <mday>*</mday>
7365     <month>*</month>
7366     <wday>*</wday>
7367     <who>root</who>
7368     <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
7369 </item>

```



```

7370      </cron>
7371      <wol/>
7372      <rrd>
7373          <enable/>
7374      </rrd>
7375      <load_balancer>
7376          <monitor_type>
7377              <name>ICMP</name>
7378              <type>icmp</type>
7379              <descr><![CDATA[ICMP]]></descr>
7380              <options/>
7381          </monitor_type>
7382          <monitor_type>
7383              <name>TCP</name>
7384              <type>tcp</type>
7385              <descr><![CDATA[Generic TCP]]></descr>
7386              <options/>
7387          </monitor_type>
7388          <monitor_type>
7389              <name>HTTP</name>
7390              <type>http</type>
7391              <descr><![CDATA[Generic HTTP]]></descr>
7392              <options>
7393                  <path></path>
7394                  <host/>
7395                  <code>200</code>
7396              </options>
7397          </monitor_type>
7398          <monitor_type>
7399              <name>HTTPS</name>
7400              <type>https</type>
7401              <descr><![CDATA[Generic HTTPS]]></descr>
7402              <options>
7403                  <path></path>
7404                  <host/>
7405                  <code>200</code>
7406              </options>
7407          </monitor_type>
7408          <monitor_type>
7409              <name>SMTP</name>

```

```

7410             <type>send</type>
7411             <descr><![CDATA[Generic SMTP]]></descr>
7412             <options>
7413                 <send/>
7414                 <expect>220 *</expect>
7415             </options>
7416         </monitor_type>
7417     </load_balancer>
7418     <widgets>
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     </unbound>
7440     <system_domain_local_zone_type>transparent</system_domain_local_zone_type>
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>

```

```
</lan>
</dhcpdv6>
<cert>
  <refid>5720a0502b277</refid>
  <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
  <type>server</type>
```

<prv>LS0tLS1CR0dJTiBQbG91bWVudF1ETWFS0tLS0tCk1JSUV2Z0lCQURBTk1Jna3Foa21HOXcwQkFRRU  
ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M01hY1kKMjN3YkNKR1htWFJWky9odVVKeFdsc3hxb3M4  
eGxiY3UyRUx6UVPjWnArc1BtQ09yaWw4SXpUS3lVQTZKaGo1YwpKdnN5U1BpK1JMWitqM0hOeXVibjsaGxzOG  
JLMjZTS1Y1M0dmVlhGak1saXhXOG0vSW1oaERUNHcWdTIA4Qnh1CjFvd0NGL3k1OE1SZVN0S1FJTEpyV1NVWFhs  
c1YrRfK5cMpgMmpZNDhRdSEliU1JZSWxLUHO1TzVtNTA5TWcwdekEKQVdeQkQzNdG5OHRUa1hROVNPb1NaClREbn  
dKTmo3cHawQnM4N1h1RDBjL2pOUFGFWSNWkem1vbKpEdDc2dmfGVwozdWdQcG5VR0FFK3ZMQzRjY25DdTcvNWRj  
dKZFyJZuWdXxdlmHmJ1A5TUt1SzdcwU1CUkxxT2pzMTN3Zy9tT3lCCmpjWUW5L314QWdNqkFBRUNN20VCQUpRRF  
pxU3duMnNTUth0SVNBtUVrUW0zcXhrb3BzdzB4cWNScmFLOEd4VmQKejBpOU1KbkZVQWFleTqVl3J1dndhZW1P  
R3RYSmZ2ai9jSnY3cmJIWGIzYkjtVW9hcDhxY0RjdnVSMmlHRUZyWQpCL3hjNvpINTlatUFabWE1VWVQZLzNjcd  
lzNVhHcHNpClnXV1T4cFFZc3Z6Mmt6ci8zMXdrQX4dSGJZWHhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHp1Zn1P  
UzAvbXlMnU5YLzVoRk1PNmFDc0x1UjZ4N1Rza2FDQU9FYlViT29qUXKkc09XewPhbEtTUWZ3WEdzdVMObXdyR2  
hmZ0NRY1B2MnE5V0Nia0VMNEZUZmRzRlZuXCHBRNG1ZSVWtnZhMY1FPMgpxSGR5c2KtJxTmJsnDIwa3h5M2FnZ1F2  
YTVqYUgyRm5LdkExR2YxY05hcGRVQz2dZUE0NzNMUWoxcExLSmRYN2JxXctMu3NVT0ZhtUz1ZG1xM2tbtzh3Qj  
lpMXhzyE1LQudM03U4dTdMZ1tU21ybnMwVVBTHMRVUDRyQXmZVFJocEqU2Z4VXsvbGVGaktjZk9xRE11TTBC  
OGttbFJnUFRmVHVPaGnWMGVkamQwK1E5Y2V1Y25kaFp3UE16TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZHnbnm  
NBRDhVYTHdZ1lFQXpzYjYzbzRBSH1YNjZkEJ6TG1zYzZxS2d2ZG4xazhVcm02N3RuK2M3NkVhSEtZT1k0Rjdh  
S0dFSklyeU0yQTJTTeLAzdm03Rmk4eGrbt1grSXd5cUx5T1VwSnZXQ012TVIKRDFpNwVFTVVoZVo2OUpOK0I3Sm  
Z2RjYrK2tHa1NHOGxaN0VLY21Uc1kzRVJxOURsSk94Nk1ROFEwMDNsTHVtQQpJZm1DWlpRSUQ1OENnWUJjamFO  
dk5obnFJOG9rWGHBUjR2c3NtNgpWb0tYU2SzcjRiVHo5MDFwOGdReXNCwkt0Cn1US2V6VThuUVZvtjNYWmVmBc  
3rVEcwYVpKOTZHKY9nNTRWmZqWTRle1VScHhUtY13QzdEx0cm5SV2NmtU2ZMM2MKS2RHN0ZuaGi0CufjNHNBSWC3  
QW5Mi9CHZJR25F51pMdnhLWTDVMX11b1NRLzcZUg1DsnFqemd6UUtC21FDZqpJQjE3RzRNWNGl3hpdGJNT

```

7512 VudmNUUjZxTzR0ekZtdG5TYWN3WlFtb2UvdUVIaGE0bU84WTBCeTNRcitVU1BCCndVR2RiUnNhdTgxcU12VUtU
7513 RGlhZGsvKy9Ud2UvVk1KbmX2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUjlhbkwzRjMKcEpUSGg4Y3FsNTdqdkRRN0
7514 FBamdyQmxrb3pOVnNMZThiWWpkcHRlMVBRs0JnQ0xDR0RlRXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1RlcZdu
7515 WjRoM3ZRODI1ZkQxbGVzVjBYdDJlcVJqeFEvSDgxMHRGd1p3cC9uSVdycnRCZlZLC1UzSThhYnpnUUtweEwrZj
7516 VadTAxY1pZVk5TU0FIUFRHYm5jb1IzbGVpYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZlFU
7517 OVFOVGJkQWJrCi0tLS0tRU5EIfBSSVZBVEUgS0VZLS0tLS0K</prv>

7518     </cert>
7519     <revision>
7520         <time>1493654529</time>
7521         <description><![CDATA[admin@10.97.67.135: /firewall_rules_edit.php made
7522 unknown change]]></description>
7523         <username>admin@10.97.67.135</username>
7524     </revision>
7525     <gateways>
7526         <gateway_item>
7527             <interface>wan</interface>
7528             <gateway>192.168.13.1</gateway>
7529             <name>GW_WAN_2</name>
7530             <weight>1</weight>
7531             <ipprotocol>inet</ipprotocol>
7532             <interval/>
7533             <descr><![CDATA[Interface wan Gateway]]></descr>
7534         </gateway_item>
7535     </gateways>
7536     <ppps/>
7537     <dyndnses/>
7538     <dnsmasq>
7539         <enable/>
7540         <custom_options/>
7541         <port>53</port>
7542         <interface/>
7543         <hosts>
7544             <host>activedirectory</host>
7545             <domain>acmefinancial.com</domain>
7546             <ip>192.168.19.10</ip>
7547             <descr/>
7548             <aliases/>
7549         </hosts>
7550     </dnsmasq>
7551 </pfSense>

```

## 2.10.5 Firewall Configuration for the Management and Monitoring Subnet

## DRAFT

```
7553 <?xml version="1.0"?>
7554 <pfSense>
7555     <version>15.4</version>
7556     <lastchange/>
7557     <theme>pfSense_ng</theme>
7558     <system>
7559         <optimization>normal</optimization>
7560         <hostname>FS-ARM</hostname>
7561         <domain>FS-ARM.gov</domain>
7562         <group>
7563             <name>all</name>
7564             <description><![CDATA[All Users]]></description>
7565             <scope>system</scope>
7566             <gid>1998</gid>
7567             <member>0</member>
7568         </group>
7569         <group>
7570             <name>admins</name>
7571             <description><![CDATA[System Administrators]]></description>
7572             <scope>system</scope>
7573             <gid>1999</gid>
7574             <member>0</member>
7575             <priv>page-all</priv>
7576         </group>
7577         <user>
7578             <name>admin</name>
7579             <descr><![CDATA[System Administrator]]></descr>
7580             <scope>system</scope>
7581             <groupname>admins</groupname>
7582             <password>$1$dSJImFph$GvZ7.1UbuWu.Yb8etC0re.</password>
7583             <uid>0</uid>
7584             <priv>user-shell-access</priv>
7585         </user>
7586         <nextuid>2000</nextuid>
7587         <nextgid>2000</nextgid>
7588         <timezone>America/New_York</timezone>
7589         <time-update-interval/>
7590         <timeservers>10.97.74.8</timeservers>
7591         <webgui>
7592             <protocol>http</protocol>
```

```

7593         <loginautocomplete/>
7594         <ssl-certref>5720a0502b277</ssl-certref>
7595         <dashboardcolumns>2</dashboardcolumns>
7596         <port/>
7597         <max_procs>2</max_procs>
7598         <nohttppreferercheck/>
7599     </webgui>
7600     <disablenatreflection>yes</disablenatreflection>
7601     <disablesegmentationoffloading/>
7602     <disablelargereceiveoffloading/>
7603     <ipv6allow/>
7604     <powerd_ac_mode>hadp</powerd_ac_mode>
7605     <powerd_battery_mode>hadp</powerd_battery_mode>
7606     <powerd_normal_mode>hadp</powerd_normal_mode>
7607     <bogons>
7608         <interval>monthly</interval>
7609     </bogons>
7610     <language>en_US</language>
7611     <dns1gw>GW_WAN</dns1gw>
7612     <dns2gw>GW_WAN</dns2gw>
7613     <dns3gw>none</dns3gw>
7614     <dns4gw>none</dns4gw>
7615     <dnsserver>10.97.74.8</dnsserver>
7616     <dnsserver>10.63.255.2</dnsserver>
7617     <serialspeed>115200</serialspeed>
7618     <primaryconsole>serial</primaryconsole>
7619     <maximumstates/>
7620     <aliasesresolveinterval/>
7621     <maximumtableentries/>
7622     <maximumfrags/>
7623     <reflectiontimeout/>
7624 </system>
7625 <interfaces>
7626     <wan>
7627         <if>em0</if>
7628         <descr><![CDATA[WAN]]></descr>
7629         <enable/>
7630         <spoofmac/>
7631         <ipaddr>192.168.13.17</ipaddr>
7632         <subnet>24</subnet>

```

```

7633         <gateway>GW_WAN_2</gateway>
7634         <ipaddrv6/>
7635         <subnetv6/>
7636         <gatewayv6/>
7637     </wan>
7638     <lan>
7639         <enable/>
7640         <if>em1</if>
7641         <ipaddr>192.168.17.1</ipaddr>
7642         <subnet>24</subnet>
7643         <ipaddrv6/>
7644         <subnetv6/>
7645         <media/>
7646         <mediaopt/>
7647         <track6-interface>wan</track6-interface>
7648         <track6-prefix-id>0</track6-prefix-id>
7649         <gateway/>
7650         <gatewayv6/>
7651     </lan>
7652 </interfaces>
7653 <staticroutes>
7654     <route>
7655         <network>192.168.19.0/24</network>
7656         <gateway>GW_VLAN19</gateway>
7657         <descr><![CDATA[Route to VLAN 2019]]></descr>
7658     </route>
7659 </staticroutes>
7660 <dhcpd>
7661     <lan>
7662         <enable/>
7663         <range>
7664             <from>192.168.17.100</from>
7665             <to>192.168.17.150</to>
7666         </range>
7667     </lan>
7668     <opt1>
7669         <enable/>
7670         <range>
7671             <from>192.168.14.100</from>
7672             <to>192.168.14.150</to>

```

```

7673             </range>
7674         </opt1>
7675         <opt2>
7676             <enable/>
7677             <range>
7678                 <from>192.168.15.100</from>
7679                 <to>192.168.15.150</to>
7680             </range>
7681         </opt2>
7682         <opt3>
7683             <enable/>
7684             <range>
7685                 <from>192.168.16.100</from>
7686                 <to>192.168.16.150</to>
7687             </range>
7688         </opt3>
7689     </dhcpd>
7690     <snmpd>
7691         <syslocation/>
7692         <syscontact/>
7693         <rocommunity>public</rocommunity>
7694     </snmpd>
7695     <diag>
7696         <ipv6nat>
7697             <ipaddr/>
7698         </ipv6nat>
7699     </diag>
7700     <bridge/>
7701     <syslog/>
7702     <nat>
7703         <outbound>
7704             <mode>disabled</mode>
7705         </outbound>
7706         <rule>
7707             <source>
7708                 <any/>
7709             </source>
7710             <destination>
7711                 <address>192.168.13.171</address>
7712                 <port>5176</port>

```



```

7713         </destination>
7714         <protocol>tcp/udp</protocol>
7715         <target>192.168.17.11</target>
7716         <local-port>5176</local-port>
7717         <interface>wan</interface>
7718         <descr><![CDATA[Mapping to ConsoleWorks]]></descr>
7719         <associated-rule-id>nat_57bf06b1aa4c21.26556306</associated-rule-
7720 id>
7721         <natreflection>purenat</natreflection>
7722         <created>
7723             <time>1472136881</time>
7724             <username>admin@192.168.13.135</username>
7725         </created>
7726         <updated>
7727             <time>1472137126</time>
7728             <username>admin@192.168.13.135</username>
7729         </updated>
7730     </rule>
7731     <separator/>
7732 </nat>
7733 <filter>
7734     <rule>
7735         <id/>
7736         <tracker>1493655499</tracker>
7737         <type>pass</type>
7738         <interface>wan</interface>
7739         <ipprotocol>inet</ipprotocol>
7740         <tag/>
7741         <tagged/>
7742         <direction>any</direction>
7743         <quick>yes</quick>
7744         <floating>yes</floating>
7745         <max/>
7746         <max-src-nodes/>
7747         <max-src-conn/>
7748         <max-src-states/>
7749         <statetimeout/>
7750         <statetype>keep state</statetype>
7751         <os></os>
7752         <protocol>tcp/udp</protocol>

```

```

7753         <source>
7754             <any/>
7755         </source>
7756         <destination>
7757             <network>lan</network>
7758             <port>514</port>
7759         </destination>
7760         <descr><![CDATA[Allow Connection to syslog in LAN]]></descr>
7761         <updated>
7762             <time>1493655499</time>
7763             <username>admin@10.97.67.135</username>
7764         </updated>
7765         <created>
7766             <time>1493655499</time>
7767             <username>admin@10.97.67.135</username>
7768         </created>
7769     </rule>
7770 <rule>
7771     <id/>
7772     <tracker>1493649494</tracker>
7773     <type>pass</type>
7774     <interface>wan</interface>
7775     <ipprotocol>inet</ipprotocol>
7776     <tag/>
7777     <tagged/>
7778     <direction>any</direction>
7779     <quick>yes</quick>
7780     <floating>yes</floating>
7781     <max/>
7782     <max-src-nodes/>
7783     <max-src-conn/>
7784     <max-src-states/>
7785     <statetimeout/>
7786     <statetype>keep state</statetype>
7787     <os/>
7788     <protocol>tcp</protocol>
7789     <source>
7790         <any/>
7791     </source>
7792     <destination>

```

```

7793             <network>lan</network>
7794             <port>1433-1434</port>
7795         </destination>
7796         <descr><![CDATA[Allow Connection to Sharepoint database-1433 and
7797 143]]></descr>
7798         <created>
7799             <time>1493649494</time>
7800             <username>admin@10.97.67.135</username>
7801         </created>
7802         <updated>
7803             <time>1493649550</time>
7804             <username>admin@10.97.67.135</username>
7805         </updated>
7806     </rule>
7807     <rule>
7808         <id/>
7809         <tracker>1493649686</tracker>
7810         <type>pass</type>
7811         <interface>wan</interface>
7812         <ipprotocol>inet</ipprotocol>
7813         <tag/>
7814         <tagged/>
7815         <direction>any</direction>
7816         <quick>yes</quick>
7817         <floating>yes</floating>
7818         <max/>
7819         <max-src-nodes/>
7820         <max-src-conn/>
7821         <max-src-states/>
7822         <statetimeout/>
7823         <statetype>keep state</statetype>
7824         <os/>
7825         <protocol>tcp</protocol>
7826         <source>
7827             <any/>
7828         </source>
7829         <destination>
7830             <network>lan</network>
7831             <port>3389</port>
7832         </destination>

```

```

7833         <descr><![CDATA[Allow Connection to RDP in LAN]]></descr>
7834         <updated>
7835             <time>1493649686</time>
7836             <username>admin@10.97.67.135</username>
7837         </updated>
7838         <created>
7839             <time>1493649686</time>
7840             <username>admin@10.97.67.135</username>
7841         </created>
7842     </rule>
7843     <rule>
7844         <id/>
7845         <tracker>1493649754</tracker>
7846         <type>pass</type>
7847         <interface>wan</interface>
7848         <ipprotocol>inet</ipprotocol>
7849         <tag/>
7850         <tagged/>
7851         <direction>any</direction>
7852         <quick>yes</quick>
7853         <floating>yes</floating>
7854         <max/>
7855         <max-src-nodes/>
7856         <max-src-conn/>
7857         <max-src-states/>
7858         <statetimeout/>
7859         <statetype>keep state</statetype>
7860         <os/>
7861         <protocol>tcp</protocol>
7862         <source>
7863             <any/>
7864         </source>
7865         <destination>
7866             <network>lan</network>
7867             <port>389</port>
7868         </destination>
7869         <descr><![CDATA[Allow LDAP Connection to LAN]]></descr>
7870         <created>
7871             <time>1493649754</time>
7872             <username>admin@10.97.67.135</username>

```

```

7873         </created>
7874         <updated>
7875             <time>1493650257</time>
7876             <username>admin@10.97.67.135</username>
7877         </updated>
7878     </rule>
7879     <rule>
7880         <id/>
7881         <tracker>1493650231</tracker>
7882         <type>pass</type>
7883         <interface>wan</interface>
7884         <ipprotocol>inet</ipprotocol>
7885         <tag/>
7886         <tagged/>
7887         <direction>any</direction>
7888         <quick>yes</quick>
7889         <floating>yes</floating>
7890         <max/>
7891         <max-src-nodes/>
7892         <max-src-conn/>
7893         <max-src-states/>
7894         <statetimeout/>
7895         <statetype>keep state</statetype>
7896         <os/>
7897         <protocol>tcp</protocol>
7898         <source>
7899             <any/>
7900         </source>
7901         <destination>
7902             <network>lan</network>
7903             <port>2389</port>
7904         </destination>
7905         <descr><![CDATA[Allow Alternate LDAP Connection to Radiant
7906     ]]></descr>
7907         <updated>
7908             <time>1493650231</time>
7909             <username>admin@10.97.67.135</username>
7910         </updated>
7911         <created>
7912             <time>1493650231</time>

```

```

7913             <username>admin@10.97.67.135</username>
7914         </created>
7915     </rule>
7916     <rule>
7917         <id/>
7918         <tracker>1493649801</tracker>
7919         <type>pass</type>
7920         <interface>wan</interface>
7921         <ipprotocol>inet</ipprotocol>
7922         <tag/>
7923         <tagged/>
7924         <direction>any</direction>
7925         <quick>yes</quick>
7926         <floating>yes</floating>
7927         <max/>
7928         <max-src-nodes/>
7929         <max-src-conn/>
7930         <max-src-states/>
7931         <statetimeout/>
7932         <statetype>keep state</statetype>
7933         <os/>
7934         <protocol>tcp</protocol>
7935         <source>
7936             <any/>
7937         </source>
7938         <destination>
7939             <network>lan</network>
7940             <port>636</port>
7941         </destination>
7942         <descr><![CDATA[Allow LDAPS Connection to LAN]]></descr>
7943         <created>
7944             <time>1493649801</time>
7945             <username>admin@10.97.67.135</username>
7946         </created>
7947         <updated>
7948             <time>1493650283</time>
7949             <username>admin@10.97.67.135</username>
7950         </updated>
7951     </rule>
7952 </rule>

```

```

7953         <id/>
7954         <tracker>1493649895</tracker>
7955         <type>pass</type>
7956         <interface>wan</interface>
7957         <ipprotocol>inet</ipprotocol>
7958         <tag/>
7959         <tagged/>
7960         <direction>any</direction>
7961         <quick>yes</quick>
7962         <floating>yes</floating>
7963         <max/>
7964         <max-src-nodes/>
7965         <max-src-conn/>
7966         <max-src-states/>
7967         <statetimeout/>
7968         <statetype>keep state</statetype>
7969         <os/>
7970         <protocol>tcp</protocol>
7971         <source>
7972             <any/>
7973         </source>
7974         <destination>
7975             <network>lan</network>
7976             <port>8000</port>
7977         </destination>
7978         <descr><![CDATA[Allow Connection to Port 8000 -Splunk
7979 Web]]></descr>
7980         <created>
7981             <time>1493649895</time>
7982             <username>admin@10.97.67.135</username>
7983         </created>
7984         <updated>
7985             <time>1493649933</time>
7986             <username>admin@10.97.67.135</username>
7987         </updated>
7988     </rule>
7989     <rule>
7990         <id/>
7991         <tracker>1493650131</tracker>
7992         <type>pass</type>

```

```

7993         <interface>wan</interface>
7994         <ipprotocol>inet</ipprotocol>
7995         <tag/>
7996         <tagged/>
7997         <direction>any</direction>
7998         <quick>yes</quick>
7999         <floating>yes</floating>
8000         <max/>
8001         <max-src-nodes/>
8002         <max-src-conn/>
8003         <max-src-states/>
8004         <statetimeout/>
8005         <statetype>keep state</statetype>
8006         <os/>
8007         <protocol>tcp</protocol>
8008         <source>
8009             <any/>
8010         </source>
8011         <destination>
8012             <network>lan</network>
8013             <port>8089</port>
8014         </destination>
8015         <descr><![CDATA[Allow Connection to Port 8089 -Splunk management
8016 por]]></descr>
8017         <updated>
8018             <time>1493650131</time>
8019             <username>admin@10.97.67.135</username>
8020         </updated>
8021         <created>
8022             <time>1493650131</time>
8023             <username>admin@10.97.67.135</username>
8024         </created>
8025     </rule>
8026     <rule>
8027         <id/>
8028         <tracker>1493650643</tracker>
8029         <type>pass</type>
8030         <interface>wan</interface>
8031         <ipprotocol>inet</ipprotocol>
8032         <tag/>

```



```

8033         <tagged/>
8034         <direction>any</direction>
8035         <quick>yes</quick>
8036         <floating>yes</floating>
8037         <max/>
8038         <max-src-nodes/>
8039         <max-src-conn/>
8040         <max-src-states/>
8041         <statetimeout/>
8042         <statetype>keep state</statetype>
8043         <os/>
8044         <protocol>tcp</protocol>
8045         <source>
8046             <any/>
8047         </source>
8048         <destination>
8049             <network>lan</network>
8050             <port>9997</port>
8051         </destination>
8052         <descr><![CDATA[Allow Connection to Port 9997 -Splunk
8053 Forwarding]]></descr>
8054         <updated>
8055             <time>1493650643</time>
8056             <username>admin@10.97.67.135</username>
8057         </updated>
8058         <created>
8059             <time>1493650643</time>
8060             <username>admin@10.97.67.135</username>
8061         </created>
8062     </rule>
8063     <rule>
8064         <id/>
8065         <tracker>1481037634</tracker>
8066         <type>pass</type>
8067         <interface>lan</interface>
8068         <ipprotocol>inet</ipprotocol>
8069         <tag/>
8070         <tagged/>
8071         <direction>any</direction>
8072         <quick>yes</quick>

```

```

8073         <floating>yes</floating>
8074         <max/>
8075         <max-src-nodes/>
8076         <max-src-conn/>
8077         <max-src-states/>
8078         <statetimeout/>
8079         <statetype>keep state</statetype>
8080         <os/>
8081         <source>
8082             <address>192.168.17.100</address>
8083         </source>
8084         <destination>
8085             <any/>
8086         </destination>
8087         <descr><![CDATA[Allow Radiant (192.168.17.100) to outside -
8088 LAN]]></descr>
8089         <created>
8090             <time>1481037634</time>
8091             <username>admin@10.97.67.155</username>
8092         </created>
8093         <updated>
8094             <time>1481037861</time>
8095             <username>admin@10.97.67.155</username>
8096         </updated>
8097         <disabled/>
8098     </rule>
8099     <rule>
8100         <id/>
8101         <tracker>1481037754</tracker>
8102         <type>pass</type>
8103         <interface>wan</interface>
8104         <ipprotocol>inet</ipprotocol>
8105         <tag/>
8106         <tagged/>
8107         <direction>any</direction>
8108         <quick>yes</quick>
8109         <floating>yes</floating>
8110         <max/>
8111         <max-src-nodes/>
8112         <max-src-conn/>

```

```

8113         <max-src-states/>
8114         <statetimeout/>
8115         <statetype>keep state</statetype>
8116         <os/>
8117         <source>
8118             <address>192.168.17.100</address>
8119         </source>
8120         <destination>
8121             <any/>
8122         </destination>
8123         <descr><![CDATA[Allow Radiant (192.168.17.100) to outside -
8124 WAN]]></descr>
8125         <created>
8126             <time>1481037754</time>
8127             <username>admin@10.97.67.155</username>
8128         </created>
8129         <updated>
8130             <time>1481037814</time>
8131             <username>admin@10.97.67.155</username>
8132         </updated>
8133         <disabled/>
8134     </rule>
8135     <rule>
8136         <id/>
8137         <tracker>1472179706</tracker>
8138         <type>pass</type>
8139         <interface>wan,lan</interface>
8140         <ipprotocol>inet</ipprotocol>
8141         <tag/>
8142         <tagged/>
8143         <direction>any</direction>
8144         <quick>yes</quick>
8145         <floating>yes</floating>
8146         <max/>
8147         <max-src-nodes/>
8148         <max-src-conn/>
8149         <max-src-states/>
8150         <statetimeout/>
8151         <statetype>keep state</statetype>
8152         <os/>

```

```

8153         <protocol>tcp</protocol>
8154     <source>
8155         <any/>
8156     </source>
8157     <destination>
8158         <any/>
8159     </destination>
8160     <descr><![CDATA[Test for comms between 2017 and 2019]]></descr>
8161     <updated>
8162         <time>1472179706</time>
8163         <username>admin@10.97.67.137</username>
8164     </updated>
8165     <created>
8166         <time>1472179706</time>
8167         <username>admin@10.97.67.137</username>
8168     </created>
8169     <disabled/>
8170 </rule>
8171 <rule>
8172     <id/>
8173     <tracker>1469130242</tracker>
8174     <type>pass</type>
8175     <interface>wan</interface>
8176     <ipprotocol>inet</ipprotocol>
8177     <tag/>
8178     <tagged/>
8179     <max/>
8180     <max-src-nodes/>
8181     <max-src-conn/>
8182     <max-src-states/>
8183     <statetimeout/>
8184     <statetype>keep state</statetype>
8185     <os/>
8186     <protocol>tcp/udp</protocol>
8187     <source>
8188         <any/>
8189     </source>
8190     <destination>
8191         <network>wanip</network>
8192         <port>80</port>

```

```

8193         </destination>
8194         <descr><![CDATA[Allow to Port 80 on Firewall WAN]]></descr>
8195         <created>
8196             <time>1469130242</time>
8197             <username>admin@192.168.17.103</username>
8198         </created>
8199         <updated>
8200             <time>1493649052</time>
8201             <username>admin@10.97.67.135</username>
8202         </updated>
8203     </rule>
8204     <rule>
8205         <id/>
8206         <tracker>1465935549</tracker>
8207         <type>pass</type>
8208         <interface>wan</interface>
8209         <ipprotocol>inet</ipprotocol>
8210         <tag/>
8211         <tagged/>
8212         <max/>
8213         <max-src-nodes/>
8214         <max-src-conn/>
8215         <max-src-states/>
8216         <statetimeout/>
8217         <statetype>keep state</statetype>
8218         <os/>
8219         <protocol>icmp</protocol>
8220         <source>
8221             <any/>
8222         </source>
8223         <destination>
8224             <any/>
8225         </destination>
8226         <descr/>
8227         <updated>
8228             <time>1465935549</time>
8229             <username>admin@192.168.17.100</username>
8230         </updated>
8231         <created>
8232             <time>1465935549</time>

```

```

8233             <username>admin@192.168.17.100</username>
8234         </created>
8235     </rule>
8236     <rule>
8237         <id/>
8238         <tracker>1461788221</tracker>
8239         <type>pass</type>
8240         <interface>wan</interface>
8241         <ipprotocol>inet</ipprotocol>
8242         <tag/>
8243         <tagged/>
8244         <max/>
8245         <max-src-nodes/>
8246         <max-src-conn/>
8247         <max-src-states/>
8248         <statetimeout/>
8249         <statetype>keep state</statetype>
8250         <os/>
8251         <protocol>tcp</protocol>
8252         <source>
8253             <any/>
8254         </source>
8255         <destination>
8256             <network>wanip</network>
8257             <port>443</port>
8258         </destination>
8259         <descr><![CDATA[Allow to Port 443 on Firewall WAN]]></descr>
8260         <created>
8261             <time>1461788221</time>
8262             <username>admin@192.168.1.2</username>
8263         </created>
8264         <updated>
8265             <time>1493649121</time>
8266             <username>admin@10.97.67.135</username>
8267         </updated>
8268     </rule>
8269     <rule>
8270         <source>
8271             <any/>
8272         </source>

```

```

8273         <interface>wan</interface>
8274         <protocol>tcp/udp</protocol>
8275         <destination>
8276             <address>192.168.17.11</address>
8277             <port>5176</port>
8278         </destination>
8279         <descr><![CDATA[NAT Mapping to ConsoleWorks]]></descr>
8280         <associated-rule-id>nat_57bf06b1aa4c21.26556306</associated-rule-
8281 id>
8282         <tracker>1472136881</tracker>
8283         <created>
8284             <time>1472136881</time>
8285             <username>NAT Port Forward</username>
8286         </created>
8287         <disabled/>
8288     </rule>
8289     <rule>
8290         <id/>
8291         <tracker>1469130278</tracker>
8292         <type>pass</type>
8293         <interface>lan</interface>
8294         <ipprotocol>inet</ipprotocol>
8295         <tag/>
8296         <tagged/>
8297         <max/>
8298         <max-src-nodes/>
8299         <max-src-conn/>
8300         <max-src-states/>
8301         <statetimeout/>
8302         <statetype>keep state</statetype>
8303         <os/>
8304         <protocol>tcp/udp</protocol>
8305         <source>
8306             <any/>
8307         </source>
8308         <destination>
8309             <any/>
8310             <port>22</port>
8311         </destination>
8312         <descr><![CDATA[Test to port 22]]></descr>

```

```

8313         <created>
8314             <time>1469130278</time>
8315             <username>admin@192.168.17.103</username>
8316         </created>
8317         <updated>
8318             <time>1472170372</time>
8319             <username>admin@192.168.13.135</username>
8320         </updated>
8321         <disabled/>
8322     </rule>
8323     <rule>
8324         <id/>
8325         <tracker>1465935564</tracker>
8326         <type>pass</type>
8327         <interface>lan</interface>
8328         <ipprotocol>inet</ipprotocol>
8329         <tag/>
8330         <tagged/>
8331         <max/>
8332         <max-src-nodes/>
8333         <max-src-conn/>
8334         <max-src-states/>
8335         <statetimeout/>
8336         <statetype>keep state</statetype>
8337         <os/>
8338         <protocol>icmp</protocol>
8339         <source>
8340             <any/>
8341         </source>
8342         <destination>
8343             <any/>
8344         </destination>
8345         <descr/>
8346         <updated>
8347             <time>1465935564</time>
8348             <username>admin@192.168.17.100</username>
8349         </updated>
8350         <created>
8351             <time>1465935564</time>
8352             <username>admin@192.168.17.100</username>

```



```

8353             </created>
8354     </rule>
8355     <rule>
8356         <type>pass</type>
8357         <ipprotocol>inet</ipprotocol>
8358         <descr><![CDATA[Default allow LAN to any rule]]></descr>
8359         <interface>lan</interface>
8360         <tracker>0100000101</tracker>
8361         <source>
8362             <network>lan</network>
8363         </source>
8364         <destination>
8365             <any/>
8366         </destination>
8367     </rule>
8368     <rule>
8369         <type>pass</type>
8370         <ipprotocol>inet6</ipprotocol>
8371         <descr><![CDATA[Default allow LAN IPv6 to any rule]]></descr>
8372         <interface>lan</interface>
8373         <tracker>0100000102</tracker>
8374         <source>
8375             <network>lan</network>
8376         </source>
8377         <destination>
8378             <any/>
8379         </destination>
8380     </rule>
8381     <separator>
8382         <wan/>
8383         <lan/>
8384         <floatingrules/>
8385     </separator>
8386     <bypassstaticroutes>yes</bypassstaticroutes>
8387 </filter>
8388 <shaper>
8389 </shaper>
8390 <ipsec/>
8391 <aliases/>
8392 <proxyarp/>

```

```

8393         <cron>
8394             <item>
8395                 <minute>1,31</minute>
8396                 <hour>0-5</hour>
8397                 <mday>*</mday>
8398                 <month>*</month>
8399                 <wday>*</wday>
8400                 <who>root</who>
8401                 <command>/usr/bin/nice -n20 adjkerntz -a</command>
8402             </item>
8403             <item>
8404                 <minute>1</minute>
8405                 <hour>3</hour>
8406                 <mday>1</mday>
8407                 <month>*</month>
8408                 <wday>*</wday>
8409                 <who>root</who>
8410                 <command>/usr/bin/nice -n20 /etc/rc.update_bogons.sh</command>
8411             </item>
8412             <item>
8413                 <minute>*/60</minute>
8414                 <hour>*</hour>
8415                 <mday>*</mday>
8416                 <month>*</month>
8417                 <wday>*</wday>
8418                 <who>root</who>
8419                 <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
8420 sshlockout</command>
8421             </item>
8422             <item>
8423                 <minute>*/60</minute>
8424                 <hour>*</hour>
8425                 <mday>*</mday>
8426                 <month>*</month>
8427                 <wday>*</wday>
8428                 <who>root</who>
8429                 <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
8430 webConfiguratorlockout</command>
8431             </item>
8432             <item>

```

```

8433         <minute>1</minute>
8434         <hour>1</hour>
8435         <mday>*</mday>
8436         <month>*</month>
8437         <wday>*</wday>
8438         <who>root</who>
8439         <command>/usr/bin/nice -n20 /etc/rc.dyndns.update</command>
8440     </item>
8441     <item>
8442         <minute>*/60</minute>
8443         <hour>*</hour>
8444         <mday>*</mday>
8445         <month>*</month>
8446         <wday>*</wday>
8447         <who>root</who>
8448         <command>/usr/bin/nice -n20 /usr/local/sbin/expiretable -v -t 3600
8449 virusprot</command>
8450     </item>
8451     <item>
8452         <minute>30</minute>
8453         <hour>12</hour>
8454         <mday>*</mday>
8455         <month>*</month>
8456         <wday>*</wday>
8457         <who>root</who>
8458         <command>/usr/bin/nice -n20 /etc/rc.update_urltables</command>
8459     </item>
8460 </cron>
8461 <wol/>
8462 <rrd>
8463     <enable/>
8464     <category>left=system-
8465 processor&right=&resolution=300&timePeriod=-
8466 1d&startDate=&endDate=&startTime=0&endTime=0&graphtype=line&in
8467 vert=true</category>
8468 </rrd>
8469 <load_balancer>
8470     <monitor_type>
8471         <name>ICMP</name>
8472         <type>icmp</type>
8473         <descr><![CDATA[ICMP]]></descr>

```

```

8474         <options/>
8475     </monitor_type>
8476     <monitor_type>
8477         <name>TCP</name>
8478         <type>tcp</type>
8479         <descr><![CDATA[Generic TCP]]></descr>
8480         <options/>
8481     </monitor_type>
8482     <monitor_type>
8483         <name>HTTP</name>
8484         <type>http</type>
8485         <descr><![CDATA[Generic HTTP]]></descr>
8486         <options>
8487             <path></path>
8488             <host/>
8489             <code>200</code>
8490         </options>
8491     </monitor_type>
8492     <monitor_type>
8493         <name>HTTPS</name>
8494         <type>https</type>
8495         <descr><![CDATA[Generic HTTPS]]></descr>
8496         <options>
8497             <path></path>
8498             <host/>
8499             <code>200</code>
8500         </options>
8501     </monitor_type>
8502     <monitor_type>
8503         <name>SMTP</name>
8504         <type>send</type>
8505         <descr><![CDATA[Generic SMTP]]></descr>
8506         <options>
8507             <send/>
8508             <expect>220 *</expect>
8509         </options>
8510     </monitor_type>
8511 </load_balancer>
8512 <widgets>

```

# DRAFT

```

8513
8514     <sequence>system_information:coll:open,gateways:coll:open,interfaces:col2:open<
8515 /sequence>
8516
8517     </widgets>
8518
8519     <openvpn/>
8520
8521     <dnshaper>
8522
8523     </dnshaper>
8524
8525     <unbound>
8526
8527         <enable/>
8528         <dnssec/>
8529         <active_interface/>
8530         <outgoing_interface/>
8531         <custom_options/>
8532         <hideidentity/>
8533         <hideversion/>
8534         <dnssecstripped/>
8535     </unbound>
8536
8537     <dhcpdv6>
8538
8539         <lan>
8540
8541             <range>
8542
8543                 <from>::1000</from>
8544
8545                 <to>::2000</to>
8546
8547             </range>
8548
8549             <ramode>assist</ramode>
8550
8551             <rapriority>medium</rapriority>
8552
8553         </lan>
8554
8555     </dhcpdv6>
8556
8557     <cert>
8558
8559         <refid>5720a0502b277</refid>
8560
8561         <descr><![CDATA[webConfigurator default (5720a0502b277)]]></descr>
8562
8563         <type>server</type>
8564
8565         <crt>LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZiVENDQkZXZ0F3SUJBZ0lCQURBTkNa3
8566 Foa2lHOXcwQkFRc0ZBRENCdERFTE1Ba0dBWVVFQmhnNQ1ZWtXgKRGpBTUJnTlZCQWdUQ1ZOMFlYUmxNUkV3RHdZ
8567 RFZRUUhFd2hNYjJOaGJHbDB1VEU0TURZR0ExVUVDaE12Y0daVApVzV6WlNCM1pXSkrImjVtYVdkMWNTtRjBiM0
8568 lnVTJWclppMVRhV2RlWldRZlEyVnlkR2xtYVdOaGRHVXhLREFTcKJna3Foa2lHOXcwQkNRRVdHV0ZrYltdsdVFI
8569 Qm1VMlZlYzJVdWJHOWpZV3hrYjIxaGFjXGFXNHhIakFjQmdOVk1JBTBQK1hCbVUyVnVjM1V0TlRjeU1HRXdOVEF5WW
8570 pJM056QWVGdzB4Tm1pBME1qY3hNVEU1TkRSYU1JRzBNUN3Q1FZRFZRUUdF
8571 d0pWVXpFT01Bd0dBWVVFQ0JNRlUzUmhkr1V4RVRBUEJnTlZCQWNUCkNFHhZMkZzYVhSNu1UZ3dOZl1lEVlFRS0
8572 V5OXDabE5sYm5ObE1lZGxZa052YmlacFozVnlZWFFJ2Y2lCVFpXeg0KTFZOCFoyNWxaQ0JEWlhKMFXWnBZMkYw
8573 WlRFb01DWUdDU3FHu01iM0RRRUUpBU1laWVdSdGFjXGFXNUFjRlplUWlclcgpaUzVzYjJOaGJHUnZiV0ZwYmpFZU1Cd0
8574 dBMVVFQXhNVMNHNWlRaVzV6WlMwMU56SXdzVEEExTURKaU1qYzNNSU1CCk1lQU5CZ2txaGtpRz13MEJBUUUVGQUFP
8575 Q0FROEFNSU1CQ2dLQ0FRUF0L085aDlnT2R5R20yTnQ4R3dpUmw1bDAKVmZ2NGJsQ2NWcGJNYXFMUE1aVzNMdG
8576 hDODBHU0dhZnJENWdqctRwZkNNMHlzbEFPaVlZK1hDYjdNa2o0dmtTMgpmbz14emNyaDUrNVlaYlBHeXR1a2ls
8577 ZWR4bjFWeFl6S1l1zYXZKdnlKb1lRMCTnTks0dkFjYnRhTUFOzjh1ZkRfClhrc1NVQ0N5YTFrbEYxNWJGZmcyUG
8578 E0eGRvMk9PNUJ5RzBrV0NKU2o4K1R1WnVkUFRJTkx3QUZnd1E5K1BQZkwKVTQxMFBVb3FFbWEwdzU4Q1RZKzZh
8579 ZEFiUEhjWGC5SFA0NFQybFNIQ2M1cUp5UTdlK3IyaFZ0N29ENloxQmdCUApyeXdlSEZwdzJ1LytYWExieEcrcD

```

```

8560 dwYXI0aHR0UFRDcm11NmFqQVVTNmpvN05kOE1QNWpZl1kzR0h2ZjhzUUlECkFRQUJvNElCaGpDQ0FZSXdDUVlE
8561 V1IwVEJBSXdbREFSQmdsZ2hrZ0JodmhDQVFfRUJBTUNCa0F3TXdzS1lJWkkKQV1iNFFnRU5CQ1lXSkU5dlpXNV
8562 RVMHdnUjJWdVpYSmhkR1ZrSUZOObGNuWmxjaUJEWl1hKMGFwXNBNBZMkYwWlRBZApCZ05WSFE0RUZnUVU3K1lLRmNp
8563 OFFVSGhTZ0xEdjhfQ3NjQ0p3QU13Z2VFR0ExVWRJd1NCMlRDQjFvQVU3K1lLcKZjaThRVUhoU2dMRHY4RUNZY0
8564 NKd0FLaGdicWtnYmN3Z2JReEN6QUpCZ05WQkFZVEFsV1RNUTR3REFZRFZRUUkKRXdWVGRHRjBaVEVSTUE4R0Ex
8565 VUVCeE1JVEc5allXeHBkSGt4T0RBMkJnTlZCQW9UTDNCbVUyVnVjMlVnZDJWaqPmJl1Wm1sbmRYSmhkRz15SU
8566 ZObGJHwXRVmMxUyMlWao1FTmxjblJwWm1sallYUmXNU2d3SmdZSktvWklodmNOCkFRa0JGaGxoWkcxGJrQnda
8567 bE5sYm5ObExteHZZMkZzWkc5dFlXbHVNUjR3SEFZRFZRUURFeFZ3WmxObGJuTmwKTFRVM01qQmhNRFV3TW1JeU
8568 56ZUNBUUF3SFFZRFZSMGxCQ1l3RkFZSut3WUJCUVVIQXdFR0NDc0dBUVVGQ0FJQwpNQXNHQTFVZER3UUVBd01G
8569 b0RBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQVFFQXJxZFpQdXd2MVZuUC82NmJDWFJ5CkVmaW1LRWlPcmtNaTB5M0
8570 9PWGtzWes1cEM2dtd6Ukl3WjEvRjYyRU93ODlUOWw4Y01ZelZOTm5Idlg0bXFPRUCUWJhRU42NEkxOHFud3Zm
8571 S2JrREZvRThMR1hSdzBkMnAyTGVmYtD4YtYvSGNHc0xHTktPbkJxb3N4ejUrQ1B3ZwpWeVRaTS9wV3p3aDdQRG
8572 c4bGdrcVc3dStlb01DNDJIBvJkOURCTmlzdfJ4RVlNMkFLQkFsZG1LYStvRUy1VUwwCm43aXpVnLZ4dHJWMTJv
8573 TTdyS1lRQ05kY00xZkVSeUwvb3ZkUnVpa0F5Wm1VVnFULldDZGo3dDdIVG9ob0RFYzEKSklkOVpPSmR2QmZLVU
8574 1sUWlELyswSvPaTaFXRDczWkdsEhTK2tOeWcladJhUjUwYjh3Wm9zQnNjSUZDa0pFbpgp0UT09Ci0tLS0tRU5E
8575 IENFUlRJRklDQVRFLS0tLS0K</crt>
8576
8577 <prv>LS0tLS1CRudJTIBQUklWQVRFIETfWS0tLS0tCk1JSUV2Z0lCQURBTkJna3Foa2lHOXcwQkFRRU
8578 ZBQVNDQktnd2dnU2tBZ0VBQW9JQkFRQzM4NzJIMkE1M0lhY1kKMjN3YkNKR1htWFJWky9odVVKeFdsc3hxb3M4
8579 eGxiY3UyRUx6UWpJWnArc1BtQ09yaWw4SxPUS3lVQTZKaGo1YwpKdnN5U1BpK1JMWitqM0hOeXV1bjdsaGxzOG
8580 JLMjZTS1Y1M0dmVlhGak1saXhXOG0vSW1oaERUNHcWdTl4Qnh1CjFvdONGL3k1OE1SZVN0S1FJTEPyV1NVWFhs
8581 c1YrRfK5cmpGMmpZNDdrSEliU1JZSWxLUHo1TzVtNTA5TWcwkEKEQVdEQkQzNDg5OHRUalhrOVNpb1NaclRebn
8582 dKTmo3cHAWQnM4Zhh1RDBJL2poUGFWSWNKem1vbkpEdDc2dmFGVwozdWdQcG5VR0FFK3ZMQzRjV25DdTcvNWRj
8583 dHZFYjZudWxxdmlHMjA5TUt1SzdwcU1CUkxxT2pzMTN3Zy9tT3lCCmpjWWU5L3l4QWdNQkFBRUNnZ0VCQUppRRF
8584 pxU3duMnNTUTh0SVNBTVUvRUW0zcXhrb3BzdZB4cWNScmFLOEd4VmQKejBpOU1KbkZVQWFletQvL3JldndhZW1P
8585 R3RYSmZ2ai9jSnY3cmJIWGIzYkYtVW9hcDhxY0RjdnVSMmlHRUZyWQpCL3hjNVpINTlaTUFabWE1VWVQLzNjC
8586 lzNVhhcHNpclNXV1I4cFFZc3Z6Mmt6ci8zMXdrQXd4SGJZWWhJVDk1CjNLRmk4VTZUM1hnU1c2eFowZHplZn1P
8587 UzAvbXlmNU5YLzVoRklPNmFDc0x1UjZ4N1RZa2FDQU9FY1ViT29qUXkKc09XeWphbEtTUWZ3WEdzdVM0bXdyR2
8588 hMZONRY1B2MnE5V0Nia0VMNEZUzmRzRlZXCHBRNGLZVWtwNzhMY1FPMgppsSGR5cTJxTmJsNDIwa3h5M2FnZ1F2
8589 YTVqYUgyRm5LdkExR2YxY05hcGRVQ2dZRUZ0NzNMUWoxcExLSmRZN2JxCMtMU3NVT0ZhTUZ1ZG1xU2ttbzh3Qj
8590 lpMXhzbElLQUd0M3U4dtdMZ1ZtU2lybnMwVVBMTMRVUDRYQXMXzVFJocEgKU2Z4VXVsbGVGaktjZk9xRE11TTBC
8591 OGttbFJnUFRmVHVPAgNwMGVkamQwK1E5Y2V1Y25kaFp3UE16TUc3TWRTSApKOG5yU2t5TFdMdWUxUVJNZNHbm
8592 NBRDhVYThDZ1lFQXpzYjYzbzRBSh1YNjZkcEJ6TG1zYzZxS2d2ZG4xazhVcm02N3RuK2M3NkVhSEtZT1k0Rjdh
8593 S0dFSk1yeU0yQTJTelAzdm03Rmk4eGRtblgrSXd5cUx5T1VwSnZXQ012TVIKRDFpNWVFTVVoZVo2OUPOK0I3Sm
8594 Z2RjYrK2tHa1NHOGxaN0VLY2lUc1kzRVJxOURsSk94Nk1ROFEwMDNsThVtQQpJZmlDW1pRSUQ1OENnWUJjamFO
8595 dk5obnFJOG9rWghBUjR2c3NtNGpWb0tYU1ZScjRiVHo5MDfWOGdReXNCWkt0Cn1US2V6VThuUVZvTjNYWmVMbC
8596 8rVEcwYVpKOTZHKy9nNTRWZmZqWTRlelVSCHhUT3QzdEx0cm5SV2NmT2ZMM2MKS2RHN0ZuaGI0cUFjNHBWSUc3
8597 QWY5Mi9CbHZJR25FS1pMdnhLWtdVMXl1Ib1NRLzczUG1DSnFqemd6UUtCZ1FDZgpJQjE3RzRnWWNGL3hpdGJNTn
8598 VudmNUUjZxtZr0ekZtdG5TYWN3W1ftb2UvdUVIaGE0bU84WTBCEtNRCitVU1BCCndVR2RiUnNhdTgxcU12VUtU
8599 RG1hZGsvKy9Ud2UvVklKbmX2TW9zS3VjTG42Y1c2eGVhR1hFc3FoUj1hbkWzRjMKcEpUSGg4Y3FNTdqdkRRN0
8600 FBamdyQmxrb3pOVnNMZThiWWpkCHRlMVBR0JnQ0xDR0R1RXNBYUxwZlRtOG44bgoyQ1h1NE52K1l3a1Rlczdu
8601 WjRoM3ZRODI1ZkQxbGVzVjBYdDJ1cVJqeFEvSDgxMHRGdlp3cC9uSVdycnRCZ1ZLC1UzSThhYnpnUUtWoeWzJj
8602 VadTAxY1pZVks5TU0FIUFRHYm5jb1IzbGVpYjNLeUVXQjdsZFBHQWpOS3UwNkd5TEkKakh5TDhadEFBRXVBZ1FU
8603 OVFOVGJkQWJrCi0tLS0tRU5EIFBSSVZBVEUgS0VZLS0tLS0K</prv>
8604
8605 </cert>
8606
8607 <revision>
8608
8609 <time>1493655499</time>
8610
8611 <description><![CDATA[admin@10.97.67.135: /firewall_rules_edit.php made
8612 unknown change]]></description>
8613
8614 <username>admin@10.97.67.135</username>
8615
8616 </revision>
8617
8618 <gateways>
8619
8620 <gateway_item>
8621
8622 <interface>wan</interface>
8623
8624 <gateway>192.168.13.1</gateway>
8625
8626 <name>GW_WAN_2</name>

```

```

8616         <weight>1</weight>
8617         <ipprotocol>inet</ipprotocol>
8618         <interval/>
8619         <descr><![CDATA[Interface wan Gateway]]></descr>
8620     </gateway_item>
8621     <gateway_item>
8622         <interface>wan</interface>
8623         <gateway>192.168.13.19</gateway>
8624         <name>GW_VLAN19</name>
8625         <weight>1</weight>
8626         <ipprotocol>inet</ipprotocol>
8627         <descr><![CDATA[Gateway to VLAN 19]]></descr>
8628     </gateway_item>
8629 </gateways>
8630 <ppps/>
8631 <dyndnses/>
8632 <virtualip>
8633     <vip>
8634         <mode>ipalias</mode>
8635         <interface>wan</interface>
8636         <uniqid>57bf05ffdcc3c</uniqid>
8637         <descr><![CDATA[VIP mapping to ConsoleWorks]]></descr>
8638         <type>single</type>
8639         <subnet_bits>32</subnet_bits>
8640         <subnet>192.168.13.171</subnet>
8641     </vip>
8642 </virtualip>
8643 </pfSense>

```

## Appendix A List of Acronyms

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