Tivoli software

IBM

Addressing Identity, Access, and Compliance Requirements

Using IBM Tivoli Identity and Access Assurance

- Introduces security solution and security management components
- Describes tangible business benefits and investment returns
- Provides customer deployment scenarios

Axel Buecker
Ryan Fanzone
Leandro Hobo
Mike Maurer

Redpaper

ibm.com/redbooks

International Technical Support Organization

Addressing Identity, Access, and Compliance Requirements Using IBM Tivoli Identity and Access Assurance

September 2010

REDP-4548-00

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (September 2010)

This edition applies to Version 1.1 of the IBM Tivoli Identity and Access Assurance offering, Product number 5724-X91.

Contents

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM web sites are provided for convenience only and do not in any manner serve as an endorsement of those web sites. The materials at those web sites are not part of the materials for this IBM product and use of those web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

Preface

Today, security is a concern for everyone, from members of the board to the data center. Each day another data breach occurs. These incidents can affect an organization's brand, investment return, and customer base. Time spent managing security incidents and managing risks can take time away from focusing on strategic business objectives. Organizations need to address security challenges by administering, securing, and monitoring identities, roles, and entitlements with efficient life-cycle management, access controls, and compliance auditing.

Those tasks include automated and policy-based user management to effectively manage user accounts and centralized authorization for web and other applications, and also enterprise, web, and federated single sign-on, inside, outside, and between organizations. Increasingly important requirements are the integration with stronger forms of authentication (smart cards, tokens, one-time passwords, and so forth) and centralizing policy-based access control of business-critical applications, files, and operating platforms.

This IBM® Redpaper™ publication describes how the IBM Tivoli® Identity and Access Assurance offering can help you address compliance initiatives, operational costs (automating manual administrative tasks that can reduce help desk cost), operational security posture (administering and enforcing user access to resources), and operational efficiencies (enhancing user productivity).

The team who wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Austin Center.

Axel Buecker is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of software security architecture and network computing technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 23 years of experience in a variety of areas related to workstation and systems management, network computing, and e-business solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in software security architecture.

Ryan Fanzone is a Certified IT Specialist and Security Solution Architect with the IBM Sales and Distribution, Software Sales organization. His specialty is working with customers to plan, design, and implement authentication and authorization solutions for complex enterprise environments. His experience includes the application of security to service-oriented architectures (SOA) and cloud computing solution models. Ryan has an MBA degree in Information Leveraged Management, and has recently completed an international assignment with the IBM Corporate Service Corp, a leadership program within the IBM Global Citizen Portfolio.

Leandro Hobo is an IT Specialist for IBM Integrated Technology Delivery in Brazil. He has worked at IBM for ten years. For the past four years, he has been involved in projects focusing on Tivoli security solutions. Previously, Leandro was a member of the WebSphere® and OS department, providing support for the WebSphere Application Server family, WebSphere Host Integration family, and Windows® 2000 Datacenter solution. He holds a Bachelor Degree in Systems Analysis from Faculdades Associadas de Sao Paulo.

Mike Maurer is an Associate IT Architect in the Server and Technology Group for IBM in Rochester, MN, U.S.A. He has six years of experience in Linux®, AIX®, Windows, Samba, Java™, Perl, and two years of experience in application software development before joining IBM. His areas of expertise include IT security, application development, system administration, and automation using various languages. He is also a Linux Professional Institute Certified (LPIC-1) Administrator.

Thanks to the following people for their contributions to this project:

Diane Sherman
International Technical Support Organization, Austin Center

Azania Abebe, Chris Bauserman, Cy Englert, Victor Russo Orlandi, Benjamin Schroeter, Ravi Srinivasan, Catherine Webb
IBM

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author - all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

`ibm.com/redbooks/residencies.html`

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

IBM Tivoli Identity and Access Assurance

This chapter provides an overview of the IBM Tivoli Identity and Access Assurance offering and introduces the individual components that are included in this offering. The chapter also presents several tangible benefits and return on investment (ROI) statements that this solution can help you achieve.

To demonstrate the cohesiveness of the individual technical solutions contained in this offering, this paper provides three distinct customer scenarios in Chapter 2, “Customer scenarios” on page 13.

1.1 Overview of the solution

IBM Tivoli Identity and Access Assurance V1.1 helps address today’s organizational security challenges by administering, securing, and monitoring identities, roles, and entitlements with efficient life-cycle management, access controls, and compliance-auditing.

IBM Tivoli Identity and Access Assurance V1.1 offers the following capabilities:

- An automated and policy-based user management solution that helps effectively manage user accounts
- Centralized authorization for web and other applications
- Enterprise, web, and federated single sign-on, inside, outside, and between organizations
- Integration with stronger forms of authentication (smart cards, tokens, one-time passwords, and so on)
- Policy-based access control of business critical applications, files, and operating platforms
- Automated monitoring, investigating, and reporting on user activity across the enterprise

The IBM Tivoli Identity and Access Assurance consists of the following individual components:

- IBM Tivoli Identity Manager V5.1
- IBM Tivoli Unified Single Sign-On V1.1
- IBM Tivoli Access Manager for Operating Systems V6.0
- IBM Tivoli Security Information and Event Manager V2.0

IBM Tivoli Identity and Access Assurance V1.1 is positioned to address several distinctive business and IT requirements that are described in the following sections.

1.1.1 Help automate the management of compliance initiatives

IBM Tivoli Identity and Access Assurance can help you understand your current posture to internal and external audit and compliance requirements by monitoring the infrastructure and user activity.

Identity management life-cycle tools can also assist in managing user access certification and recertification, and user provisioning as a vital part of the overall compliance posture.

1.1.2 Help with operational efficiency and cost reduction

With staff costs becoming a burden, operational efficiency is key to a successful business. There is a need to improve user productivity by helping ensure that users of IT systems have the necessary access and rights to effectively carry out their roles, in addition to having access to the relevant IT systems. IBM Tivoli Identity and Access Assurance provides the necessary tools for the following deployment initiatives:

- Portal and Microsoft® SharePoint deployments
- Single sign-on deployments
- User provisioning deployments
- Enterprise resource planning (ERP) deployments and upgrades
- Organizational restructuring

1.1.3 Help address security

With more focus being placed on data breaches and consequently the loss of reputation and confidence in the business, the need for being able to detect and react to these situations is important, because the cost to the organization can be huge. IBM Tivoli Identity and Access Assurance provides the tools that can help you address these security issues:

- Response to security incidents
- Entitlement management projects
- Privileged user monitoring
- Password management
- Employee ID projects

1.1.4 Help improve user productivity and cost reduction

With individual users having to juggle and remember many more credentials to access their systems to do their jobs, efficiency in using IT systems is a key concern and it can be the cause of frustration and lost productivity. Often, a prolonged amount of time and cost is spent by the IT support group to respond to password-related requests. IBM Tivoli Identity and Access Assurance addresses these concerns by providing the following features:

- Single sign-on functionality
- Self-service access request and maintenance functionality
- Mobile banking and payments integration

To put the technical breadth of this bundle in context, we highlight three distinct customer problems that components of IBM Tivoli Identity and Access Assurance are able to solve (see Chapter 2, “Customer scenarios” on page 13). However, we first briefly describe each of the components included in the offering and highlight key business issues they can address.

1.2 IBM Tivoli Identity and Access Assurance components

As mentioned in the introduction, IBM Tivoli Identity and Access Assurance V1.1 consists of the following products:

- IBM Tivoli Identity Manager V5.1
- IBM Tivoli Access Manager for Operating Systems V6.0
- IBM Tivoli Security Information and Event Manager V2.0
- IBM Tivoli Unified Single Sign-On V1.1

1.2.1 IBM Tivoli Identity Manager V5.1

Tivoli Identity Manager provides an automated and policy-based solution that can help effectively manage user accounts, access permissions, and passwords from creation to termination in IT environments. It can automate the processes of creating and provisioning or de-provisioning user privileges across heterogeneous IT resources throughout the entire user life cycle.

Tivoli Identity Manager can help increase user efficiency, reduce IT administration costs, and manage compliance with your security policies with centralized user account maintenance (including self-service interfaces), delegated administration, automated approvals processing, periodic revalidation of user access rights, documentation of controls, and other standard reports. Tivoli Identity Manager can help resolve how business users view their IT resources and the actual IT implementation of user access rights, maximize productivity of the various groups of users involved in identity management, and accelerate and simplify system deployment and ongoing administration.

More information: See the following resources for in-depth design, product components, and deployment information about IBM Tivoli Identity Manager:

- *Identity Management Design Guide with IBM Tivoli Identity Manager*, SG24-6996
- Part 3 “Managing identities and credentials” in *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014

1.2.2 IBM Tivoli Access Manager for Operating Systems V6.0

Employees, not hackers or viruses, generally present the major threat to an organization's IT security and information assets. Internal users account for the majority of cyber theft. They know where the most valuable data resides and at which times it is most vulnerable.

Tivoli Access Manager for Operating Systems provides a security server engine for UNIX®, Red Hat, SUSE Linux, and Linux for System z® operating systems. This engine provides security services that can be applied to one or more users of a UNIX system. However, conventional UNIX operating system design requires a *super user ID*[1] for most administrative operations. This design can open the UNIX platform to vulnerabilities as a super user gains access capabilities with few, if any, restrictions. Also, with the complexity of managing access to the UNIX operating system from multiple vendors, UNIX security can become as expensive as it is risk-laden. Tivoli Access Manager for Operating Systems offers a policy-based solution to address this security issue with UNIX and Linux. It also provides interoperability within the security and management portfolio offered by IBM.

Tivoli Access Manager for Operating Systems intercepts system calls and uses the identity of the accessor to make a policy decision about whether the access should proceed. This approach is achieved through standard interfaces into the operating system that avoid the need for kernel recompiles or complicated install mechanisms. At the same time, this interaction with the operating system provides high levels of policy control.

Tivoli Access Manager for Operating Systems introduces a comprehensive audit data capture and reporting framework to help address audit and governance requirements for production in UNIX and Linux systems.

More information: Additional information about IBM Tivoli Access Manager for Operating Systems is in Chapter 12 "Access Manager for Operating Systems" in *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014.

1.2.3 IBM Tivoli Security Information and Event Manager V2.0

Using its W7 methodology, Tivoli Security Information and Event Manager can help you to better read and interpret native log data, which can be complex at times. With this available information, you can perform the following tasks:

- Quickly assess user behavior, system activity, and security information across all platform types.
- Compare log entries to your baseline policy to help pinpoint and minimize security problems.
- Deliver reporting to support auditors' evidence requests and security managers' investigational requirements without the need for expensive platform experts.
- Rapidly respond to incidents by setting actions and alerts about privileged user activity, and allowing administrators to perform their jobs.

More information: For more in-depth design, product components, and deployment information about IBM Tivoli Security Information and Event Manager, see *IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager*, SG24-7530.

[1] A super user ID usually is a single predefined ID, also called a *root* user, with a unique level of privileges that allows an administrator to bypass standard UNIX or Linux security checks.

1.2.4 IBM Tivoli Unified Single Sign-On V1.1

The IBM Tivoli Unified Single Sign-On offering enables you to realize the combined benefits of three leading single sign-on products:

- IBM Tivoli Access Manager for Enterprise Single Sign-On V8.1 (Suite component)
- IBM Tivoli Federated Identity Manager V6.2.1
- IBM Tivoli Access Manager for e-business V6.1.1

These are breifly described in the following sections.

IBM Tivoli Access Manager for Enterprise Single Sign-On V8.1

Tivoli Access Manager for Enterprise Single Sign-On allows organizations to automate access to corporate information, strengthen security, and enforce compliance at the enterprise end-points.

With Tivoli Access Manager for Enterprise Single Sign-On product, organizations can efficiently manage business risk, achieve regulatory compliance, decrease IT costs, and increase user efficiency. Organizations do not have to choose between strong security and convenience.

Tivoli Access Manager for Enterprise Single Sign-On delivers the following capabilities, without requiring changes to the existing IT infrastructure:

- Strong authentication for all user groups
- Enterprise single sign-on with workflow automation
- Comprehensive session management ability
- User-centric access tracking for audit and compliance reporting
- Secure remote access for easy, secure access—any time and anywhere
- Integration with user provisioning technologies

More information: For more in-depth design, product components, and deployment information, see *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350.

IBM Tivoli Access Manager for e-business V6.1.1

The Tivoli Access Manager for e-business product is a web single sign-on, authentication and authorization solution for corporate web applications. Tivoli Access Manager for e-business allows you to control user access to protected information and resources that are being accessed through the web. By providing a centralized, flexible, and scalable access control solution, Tivoli Access Manager for e-business allows you to build secure and easy-to-manage network-based applications and e-business infrastructures.

Tivoli Access Manager for e-business supports web single sign-on, authentication, authorization, data security, and resource management capabilities. You use Tivoli Access Manager for e-business in conjunction with standard Internet-based applications to implement highly secure and well-managed access control to applications and data located in your private network. Access can be from within the private network, from the Internet, or from an extranet.

Tivoli Access Manager for e-business provides the following services:

- Authentication services

  The Tivoli Access Manager for e-business *authentication service* uses a wide range of built-in authenticators and supports external authenticators.

- Authorization services

  The Tivoli Access Manager for e-business *authorization service*, accessed through a standard authorization application programming interface (API), provides permit/deny decisions for access requests for native Tivoli Access Manager for e-business servers and other applications.

  The authorization services, together with resource managers, provide a standard authorization mechanism for business network systems.

Tivoli Access Manager for e-business can be integrated into existing and emerging infrastructures to provide secure, centralized policy management capability. Tivoli Access Manager for e-business integrates with IBM WebSphere Application Server, IBM WebSphere Portal, IBM Tivoli Identity Manager, IBM Tivoli Access Manager for Enterprise Single Sign-On, and IBM Tivoli Federated Identity Manager to form a complete *Enterprise Identity Management* solution.

More information: See the following resources for in-depth design, product components, and deployment information about IBM Tivoli Access Manager for e-business:

- *Deployment Guide Series: IBM Tivoli Access Manager for e-business V6.0*, SG24-7207
- Chapter 6 "Access Manager for e-business" in *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014

IBM Tivoli Federated Identity Manager V6.2.1

A *federation* is considered a group of two or more trusted business partners bound by business and technical agreements that allow a user from one federation partner (participating company) to seamlessly access resources from another partner in a secure and trustworthy manner. In a federated business model (in which services are being federated, or shared, with business partners), an organization shares identity data about its users with trusted partners. Sharing identity data enables a partner-organization to obtain information about a third-party identity (for example, customer, supplier, or client employee) from that user's home organization. This approach eliminates the need for the partner-organization to create and manage identity data for the third-party user.

This federation approach spares the user from having to register at another organization's site and consequently having to remember yet another login ID and password, and can instead use the identity issued by the user's home organization to access the other organization's web site and applications. This technique can result in improved integration, communication, and information exchange among suppliers, business partners and customers, using IT systems and procedures to help lower overall costs, improve productivity, and maximize efficiency in business operations.

Tivoli Federated Identity Manager is a complete solution that offers federated web single sign-on and allows organizations to participate in a federation. It provides organizations with the maximum flexibility by supporting all three major federation standards: *Liberty*, *WS-Federation*, and *Security Assertion Markup Language (SAML)*. Tivoli Federated Identity Manager supports user-centric identities such as OpenID, Information Card Profile using Microsoft CardSpace, and Project Higgins as identity selectors.

In addition, Tivoli Federated Identity Manager enables compliance reporting in service-oriented architecture (SOA) environments.

More information: See the following resources for more information about IBM Tivoli Federated Identity Manager:

- *Propagating Identity in SOA with Tivoli Federated Identity Manager*, REDP-4354
- *Federated Identity and Trust Management*, REDP-3678
- *Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions*, SG24-6394
- Part 4 “Managing Federations” in *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014

1.2.5 Included IBM middleware products

All of the previously mentioned IBM products can use underlying middleware technology from IBM that is provided for use in conjunction with the components of the IBM Tivoli Identity and Access Assurance, at no cost. The precise support requirements and license details can be obtained in the individual product documentation:

- IBM DB2®
- IBM Tivoli Directory Server
- IBM Tivoli Directory Integrator
- IBM WebSphere Application Server
- IBM Global Security Kit
- IBM Java Runtime

Many third-party database, directory, Java, and application server middleware components are also supported.

1.3 Tangible benefits and return on investment (ROI)

With an increasing number of users, applications, and access points, organizations face the challenge of managing identities across the user life cycle, providing convenient access to a variety of data and systems while ensuring strong and compliant security. IBM Tivoli Identity and Access Assurance can help organizations ensure that the right users have access to the right information in a timely manner, providing comprehensive identity management, access control management, and user compliance auditing capabilities. The solution centralizes and automates the management of users, then closes the identity and access loop, providing industry-leading capabilities not only for assigning and enforcing user access rights, but also for monitoring user activity and for detecting and correcting situations that are out of compliance with security policy.

This section describes the business drivers, their effect on the IT infrastructure, and how the IBM Tivoli Identity and Access Assurance V1.1 offering can be a major player in improving the business solutions in the following areas:

- Identity management: Enrolling new users and assigning them appropriate access rights, changing user roles and modifying privileges, and terminating user access rights at the end of the user life cycle
- Access management: Providing secure authentication of users, including single sign-on capabilities, and enforcing user access policies after the user has been authenticated

- User compliance auditing: Monitoring, auditing, and reporting on user activity, helping organizations to facilitate compliance with corporate policies and regulatory mandates, and reducing the risk of internal threats by monitoring users for abnormal behavior

With the Tivoli Identity and Access Assurance, IBM combines the capabilities of the IBM identity and access management product portfolio, integrating them in a single solution that addresses the entire user life cycle:

- The solution can help organizations improve services by enabling collaboration through role-based portals, facilitating the quick roll-out of new services and applications, and enabling single sign-on.
- Tivoli Identity and Access Assurance can help organizations reduce costs for managing accounts, groups, policies, credentials and access rights throughout the user life cycle by providing a single-vendor solution that reduces the total-cost-of-ownership (TCO) and complexity while giving users quick access to the resources they need.
- Finally, organizations can better manage risk with the integrated support the solution provides for compliance efforts, including centralized and automated audit compliance reporting, robust user activity monitoring, and strong password policy enforcement capabilities.

Note: Alinean Inc. is a leading provider of on-demand sales tools and related services. IBM has partnered with Alinean to create the IBM Business Value Analyst to help customers financially justify IBM solutions by focusing on business value and ROI. The Business Value Analyst is a tool available to Tivoli sales teams through Extreme Leverage and IBM Business Partners through the Tivoli Knowledge Center. For more information about Alinean, go to the following website:

http://www.alinean.com/

1.3.1 Impact on business drivers

This section examines the effect on the business drivers.

- How to avoid lost productivity as a result of password resets

  Because users only need to remember one single password when signing in to their workstations, Tivoli Access Manager for Enterprise Single Sign-On can improve user productivity. By providing a self-service password reset function Tivoli Access Manager for Enterprise Single Sign-On can reduce help desk calls for password resets, and by that save time for the users in waiting for password resets.

  By providing a web-based password reset facility in combination with its centralized user life-cycle management and password synchronization capabilities, IBM Tivoli Identity Manager can further increase the cost and time savings.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be in the range of 40 - 60%.

- How to save on managing user access provisioning to critical resources.

  Tivoli Identity Manager's workflow-enabled access provisioning engine and the Tivoli Access Manager for e-business common security infrastructure can enable organizations to administer user access privileges more easily, giving users quicker access to critical resources.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be in the range of 23 - 47%.

- How to minimize costly insider threats and damaging mistakes by providing user behavior audit trails

  According to various security-related industry reports, 80% of insider threats are caused by privileged or technical users. IBM Tivoli Security Information and Event Manager adds a *camera lens* to your network by collecting and allowing you to *view* the audit trail logs as evidence of user behavior. When insiders know you are watching, the chance of data theft can be reduced and the ability to understand, avoid, and remediate mistakes improves.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be approximately 15%.

- How to improve time-to-market by reducing application development effort

  By eliminating the need to code security logic into individual applications, IBM Tivoli Access Manager for e-business can reduce application development effort, and speeds application deployment.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be approximately 20%.

1.3.2 Impact on IT operations

This section examines the effect on the IT operations.

- How to save on help desk calls for resetting passwords

  IBM Tivoli Access Manager for Enterprise Single Sign-On can deliver single sign-on functionality for many systems and applications throughout an organization. This feature can greatly reduce the number of help desk calls that are related to password problems.

  IBM Tivoli Identity Manager can further reduce help desk calls for password resets by providing a web based self-service password reset facility.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be in the range of 40 - 60%.

- How to automate log management, including formatting and processing for compliance

  Tivoli Security Information and Event Manager can automate log management by allowing for universal collection, storage, retrieval, and investigation of security log data. In addition it can automatically format and process logs for compliance and investigatory reports.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be approximately 40%.

- How to simplify the management of user-identity life cycles

  IBM Tivoli Federated Identity Manager, IBM Tivoli Identity Manager, and IBM Tivoli Access Manager for Enterprise Single Sign-On provide a common infrastructure for managing user identity information internally or using standard LDAP user repositories.

  IBM Tivoli Access Manager for e-business integrates with standard LDAP user repositories, and IBM Tivoli Identity Manager, for simplifying the management of user identities across multiple applications.

  IBM Tivoli Federated Identity Manager provides a secure infrastructure for provisioning users across domain and organization boundaries. In addition, Tivoli Federated Identity Manager simplifies user management and audit logging in federated environments.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be in the range of 20 - 38%.

- How to provide comprehensive compliance management and reporting

  IBM Tivoli Security Information and Event Manager can automate log management by allowing for universal collection, storage, retrieval, and investigation of security log data. It then automatically formats and processes logs for compliance and investigatory reports. Modules for specific regulations, such as SOX[2], HIPAA[3], ISO[4], and GLBA[5], can save additional time in automating compliance-related reporting.

  By providing unified audit for UNIX and Linux authorization, and providing consolidation of auditing between itself and the UNIX and Linux audit logs, IBM Tivoli Access Manager for Operating Systems can improve the efficiency of access control auditing across UNIX and Linux systems.

  IBM Tivoli Federated Identity Manager, IBM Tivoli Access Manager for Enterprise Single Sign-On, and IBM Tivoli Access Manager for e-business can further simplify the auditing of users' unified authentication and authorization by providing audit logs to Tivoli Security Information and Event Manager.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be in the range of 15 - 25%.

- How to reduce the effort for managing access privileges

  IBM Tivoli Identity Manager, IBM Tivoli Access Manager for e-business, and IBM Tivoli Access Manager for Operating Systems provide an infrastructure for a wide range of web and enterprise applications and operating systems, greatly reducing the effort required for administering access privileges.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be in the range of 8 - 24%.

- How to save on security related application development tasks

  IBM Tivoli Access Manager for e-business support for multiple application programming interfaces, including JAAS, J2EE, and .NET can help reduce the need to code security logic into individual applications.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be approximately 17%.

- How to simplify and centralize credential and policy management

  IBM Tivoli Security Information and Event Manager enables you to specify W7 rules, which can look at details about *who* can do *what*, *when*, *where*, *where from* and *where to* so that acceptable use and change management policies can be monitored and enforced automatically. In addition, IBM Tivoli Federated Identity Manager, IBM Tivoli Identity Manager, IBM Tivoli Access Manager for e-business, IBM Tivoli Access Manager for Operating Systems, and IBM Tivoli Access Manager for Enterprise Single Sign-On can simplify and centralize user ID creation, password and other credential management, and access control.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be in the range of 7 - 15%.

[2] Sarbanes-Oxley Act (SOX): http://www.sarbanes-oxley.com/
[3] Health Insurance Portability and Accountability Act (HIPAA): http://www.hhs.gov/ocr/privacy/index.html
[4] ISO/IEC 27001:2005 security standards: http://www.iso.org/iso/catalogue_detail?csnumber=42103
[5] Gramm-Leach Bliley Act (GLBA): http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

- How to provide log forensics to help investigate user behavior

  IBM Tivoli Security Information and Event Manager ubiquitous log collection, forensics, and management capability allows you to store, retrieve, and investigate logs for user behavior across any server, application, database or device.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be approximately 15%.

- How to automate aspects of pre-audit preparation

  Audits can costs hundred of thousands of dollars to prepare for. IBM Tivoli Security Information and Event Manager can automate many aspects related to gathering log files, generating compliance reports, demonstrating evidence of meeting regulations and standards, enabling audit investigations, and more.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be approximately 15%.

- How to reduce cost and time spent on the actual audit

  While auditors are on site, they might ask for significant volumes of data and reports. For security audits, IBM Tivoli Security Information and Event Manager can automate the collection of log information and reporting against compliance.

  The Business Value Analyst tool from Alinean reports an organization's cost savings can be approximatelyt 15%.

1.4 Conclusion

The IBM Tivoli Identity and Access Assurance is a comprehensive identity life-cycle management and access control offering. It interoperates with a broad set of repositories, can handle large volumes of concurrent administrative activities, and enables automation of business process workflows, improving administrative efficiency and minimizing costly errors.

User activity data captured through automated auditing can flow seamlessly into the administration and compliance function, closing the identity and access loop and allowing organizations to remediate exposures and threats immediately.

2

Customer scenarios

This chapter describes three distinct customer scenarios, each one focusing on a specific business or technical requirement. It begins with an overview of the challenges these organizations are facing. The scenarios are as follows:

- Single sign-on and centralized user ID management for employees
- Log and access management for audit readiness
- Accessing services from external business partners

This chapter can help answer the following questions:

- How can the IBM Tivoli Identity and Access Assurance offering best be used to address these various requirements?
- What is the preferred technical approach and which component should be implemented first?

2.1 Single sign-on and centralized user ID management for employees

In this first scenario, a large retailer wants to address the following requirements:

- Reduce escalating operational costs for identity life-cycle management.

  The retail organization has deployed a large number of applications. Today, user IDs are still being managed manually for these individual applications. With fast-paced changes in the employee landscape, the costs of properly maintaining the user population is getting out of control.

  A centralized mechanism is needed to remedy the situation and provide a consistent approach to provision, manage, and deprovision user IDs when the time comes.

- Reduce escalating operational costs for calls related to resetting passwords.

  Because of the amount of individually managed applications, a user must remember a large number of user ID and password combinations. Combining that issue with the task of adding new employees, a high workload for the user help desk is created.

A self-service functionality is required to empower users to manage and reset their passwords without the explicit intervention of help desk personnel.

- Provide a homogeneous workplace experience for employees to increase productivity and reduce frustration over a number of distributed kiosk-type workstations.

  Instead of being prompted to log on to individual applications several times a day (because of timeout and inactivity properties) the employees should be able to access all IT-related resources by providing one single user ID and password combination on a distributed number of Microsoft Windows-based kiosks throughout the retail floor, and in individual office environments.

  A single sign-on infrastructure is needed to manage access profiles for individual applications on a per-user base. These individual user profiles must be accessible from a variety of workstations and kiosks throughout the infrastructure.

To address these requirements, the retail organization has decided to implement the project in three phases:

- Phase 1: Implementing an automatic provisioning service
- Phase 2: Implementing password-reset self-service
- Phase 3: Implementing enterprise single sign-on

2.1.1 Phase 1: Implementing an automatic provisioning service

To address the requirement of provisioning user IDs to multiple services, the retailer selects the IBM Tivoli Identity Manager component that is included in the IBM Tivoli Identity and Access Assurance offering.

Figure 2-1 on page 15 introduces the following services:

- The *Tivoli Identity Manager server* application is being deployed within the Management Network zone[1]. The diagram shows two stacked Tivoli Identity Manager (abbreviated as TIM in the figure) server components indicating that in this case they are being deployed on an application server cluster to provide high availability. The Tivoli Identity Manager server is accessing a *database server cluster* and an *LDAP master directory* to store operational-related and user-related data. The LDAP directory physical layout also provides an LDAP Replica, that, together with the clustered database server and the clustered Tivoli Identity Manager server, provides a highly available deployment.
- The *Tivoli Identity Manager web based user interface* (abbreviated as TIM UI in the figure) is deployed on existing web application server clusters in the Production Network zone, one server that is facing external users and another one for internal users. Both application server clusters are being accessed through Web Security Servers that provide access control to application resources.
- An *IBM Tivoli Directory Integrator* (abbreviated as TDI in the figure) server is being deployed in the Production Network zone to handle the *HR data feed* procedures to feed user related data into Tivoli Identity Manager. The HR database application has been identified to be the authoritative data source for user-related information.
- A Tivoli Identity Manager adapter infrastructure is being put in place within the Production Network zone to manage user-related data on the managed resources, such as applications, system resources, and so on.

[1] For more detail about network zones, see *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014.

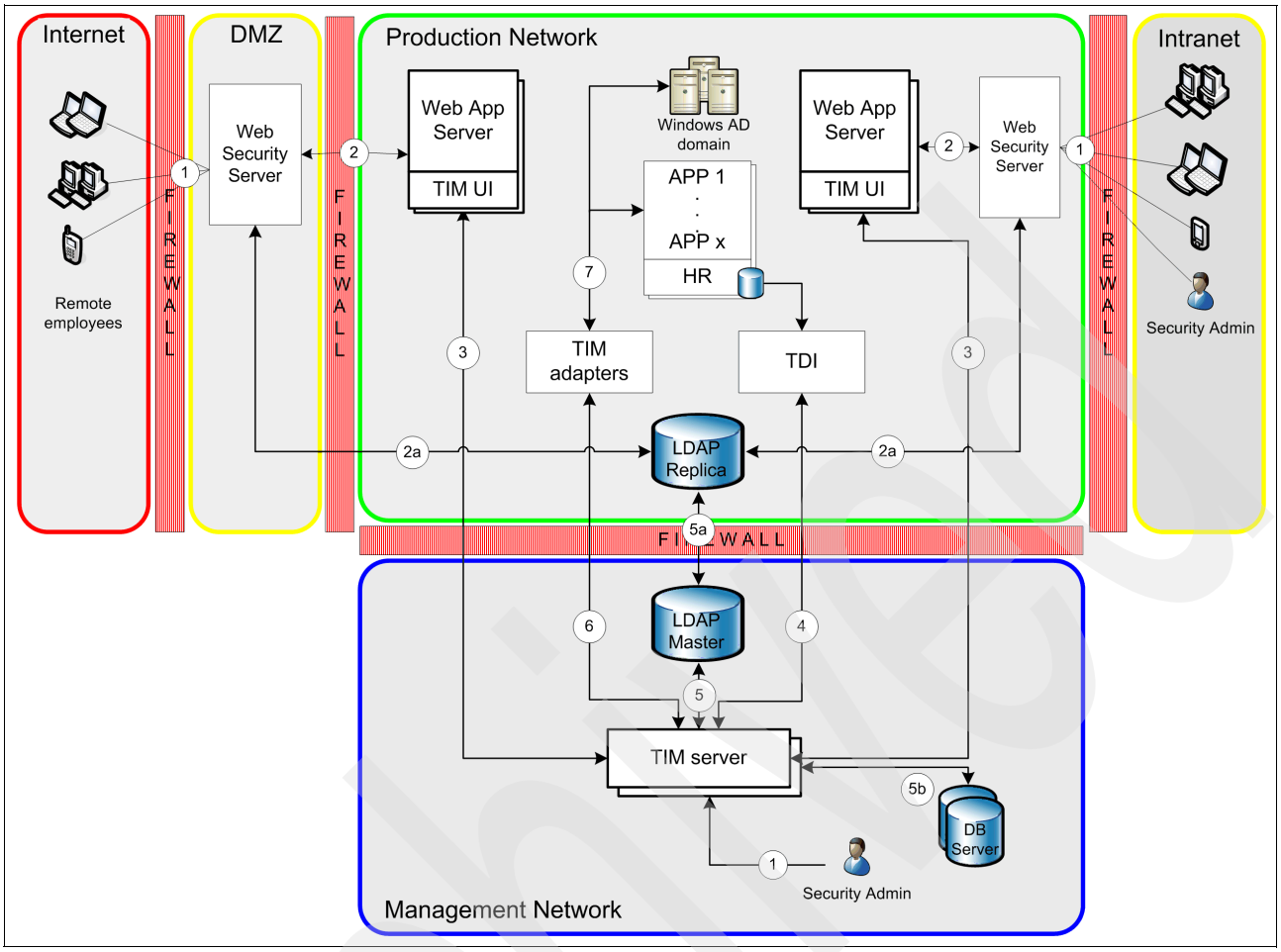

Figure 2-1 Phase 1 implementation architecture

With Tivoli Identity Manager In the first phase, the retailer can address the following issues:

- Automate user account administration operations, including creation, modification, suspension, and password change. These operations must be executed correctly and in a timely manner.
- Automate and centralize administrative operations that are related to user account management to reduce the cost of managing users and their accounts.
- Enforce the corporate security policy for all user accounts and their attributes, access rights, and password rules. User accounts that are inconsistent with the policy are generally not allowed.

No external use for this project phase: Although the retailer is not including identity life-cycle management for customers or any other external party at this time, the deployment architecture diagrams show that the Internet-facing web application server side is included in the Tivoli Identity Manager implementation. The reason is because several employees (office staff, management, administration, and so on) are supposed to be able to access the resources from a remote location, such as a home office for example.

For a successful implementation, the retailer follows four steps:

1. Prepare for tasks that must be completed before Tivoli Identity Manager can be committed to production. These tasks include system installation and verification of the correct operation of the components. In this initial phase, the retailer also creates and tests the *HR feed* process, defines *managed resources* along with the deployment of the necessary *adapters*, and runs a *reconciliation* including *orphan account cleanup*.

   The initial HR feed reads existing employee data and creates Tivoli Identity Manager people entries for each of them. This process also creates a Tivoli Identity Manager account for each of them. The HR feed process is being configured in a way that new people entries can be automatically created for newly hired employees, and that accounts are suspended on termination by using the reconciliation feature.

   Next, the managed resources are defined, for example, several web applications, Windows domain user accounts, and so on. Using the appropriate adapters to communicate with the managed resources, the reconciliation process then imports existing user accounts from the managed resources and tries to map those to the users by using specific policies. If the reconciliation process is not able to map all accounts to existing users, the result is a number of orphan accounts, which are accounts that cannot be automatically associated with existing real people. These orphan accounts must now be manually mapped to users to create an owner relationship.

2. Implement account management functionality. In this step, the retailer defines how common accounts will be automatically created in Tivoli Identity Manager when a new person is created by the HR identity feed. This step also includes the handling of account suspension when a person is terminated.

   Up to this point the tasks are largely invisible to the general user population and, therefore, do not require any training.

3. Implement additional Tivoli Identity Manager functionality. This phase addresses the challenge/response functionality for password resets, account maintenance through the Tivoli Identity Manager Web Self-Service interface, delegated administration, and approval workflows. In addition, regional accounts are automatically granted or suspended, based on transfer in the HR feed, and compliance alerts are generated. The deployment of the Tivoli Identity Manager Self-Service user interface is separately described in 2.1.2, “Phase 2: Implementing password-reset self-service” on page 18.

4. Enable full Role Based Access Control (RBAC) and define organization-wide roles and provisioning polices for those roles. In addition to defining roles and provisioning policies, a self-service interface is provided to request role changes.

More information: For further details, see *Identity Management Design Guide with IBM Tivoli Identity Manager*, SG24-6996.

The following sections (“Data flow” on page 16 and “Implementation steps” on page 18) provide a high-level description of data flow and implementation.

Data flow

As you read through the following data flow example, refer to Figure 2-1 on page 15:

1. Security administrators access the Tivoli Identity Manager UI application through their web browser to administer the Tivoli Identity Manager functionality.

   To manage and maintain the physical Tivoli Identity Manager server deployment, security administrators have to access the Tivoli Identity Manager servers that are located in the Management Network zone directly.

All other users are also able to access the Tivoli Identity Manager UI application using their browsers when they have a Tivoli Identity Manager account. They can see only their account-related information.

2. All internal and external web-based access is routed through an existing Web Security Server, which redirects the requests to an application server with the Tivoli Identity Manager UI application installed.

   Web Security Servers: At the retailer, the implemented Web Security Server is a WebSEAL server that is part of Tivoli Access Manager for e-business. Tivoli Access Manager for e-business has been previously deployed and is not part of this phase. However, Tivoli Access Manager for e-business is a part of the Tivoli Identity and Access Assurance solution bundle and can be implemented as part of your project.

   a. Upon a user's request to access this application, the Web Security Servers authenticate the users through an LDAP server. Access is allowed only if the user is successfully authenticated and has been granted sufficient access privileges. A single sign-on protocol provides the user's credentials to the Tivoli Identity Manager UI application.

      Single sign-on protocol: The single sign-on protocol that provides the user's credentials to the Tivoli Identity Manager UI application is also an essential function of Tivoli Access Manager for e-business.

3. The Tivoli Identity Manager UI application communicates with the Tivoli Identity Manager server. Based on the user's credentials (for example, administrator or help desk personnel) certain administrative application functions are either accessible or not.
4. Tivoli Identity Manager uses *IBM Tivoli Directory Integrator* to implement its HR data feed functionality. This operation can be scheduled, manually invoked, or triggered by specific events.
5. After the HR information has been retrieved through Tivoli Directory Integrator (for example, employees being hired and others leaving the company), Tivoli Identity Manager manages the person records within the LDAP Master database, either creating new or suspending entries. Figure 2-1 on page 15 shows 5a and 5b:
   a. The LDAP Master server replicates information instantaneously to the LDAP Replica server for high availability reasons.
   b. Operational data (for example, identity management workflow status) is stored on within the database server cluster.
6. Tivoli Identity Manager uses adapters to enforce its provisioning policies. Tivoli Identity Manager submits operations (either create, delete, or modify) for user accounts on managed resources following several other operational policies.
7. Tivoli Identity Manager adapters handle the individual user ID operations on the managed resources. The results of these operations are stored within the Tivoli Identity Manager database server. The information about the provisioned users is stored within the LDAP server.

Implementation steps

The provisioning implementation steps are as follows:

1. Install Tivoli Identity Manager and its required middleware components.
2. Define any custom person types if required.
3. Define the Organization tree (your organization structure).
4. Create an identity feed and validate the feed data.
5. Install Tivoli Identity Manager adapters and define managed resources.
6. Execute reconciliations for each installed adapter to create a list of accounts and map those to the owners.
7. Clean up any orphan accounts left over by the reconciliations (for example, as required for SOX compliance).
8. Harden your Tivoli Identity Manager servers and components. For example, set UNIX or Linux permissions, secure access to LDAP and HR data, secure communication between components using Secure Sockets Layer (SSL), and so on.
9. Enable the automatic creation of common accounts (such as email and Windows) for new employees as they are created in Tivoli Identity Manager.
10. Enable automatic suspension of accounts when the account owner is no longer an active employee.

2.1.2 Phase 2: Implementing password-reset self-service

To reduce the escalating operational costs for help desk calls that are related to resetting passwords, the retailer chose to implement Tivoli Identity Manager's self-service password-reset service. Figure 2-2 on page 19 shows the retailer's setup for the Tivoli Identity Manager self-service password-reset application on the web application server.

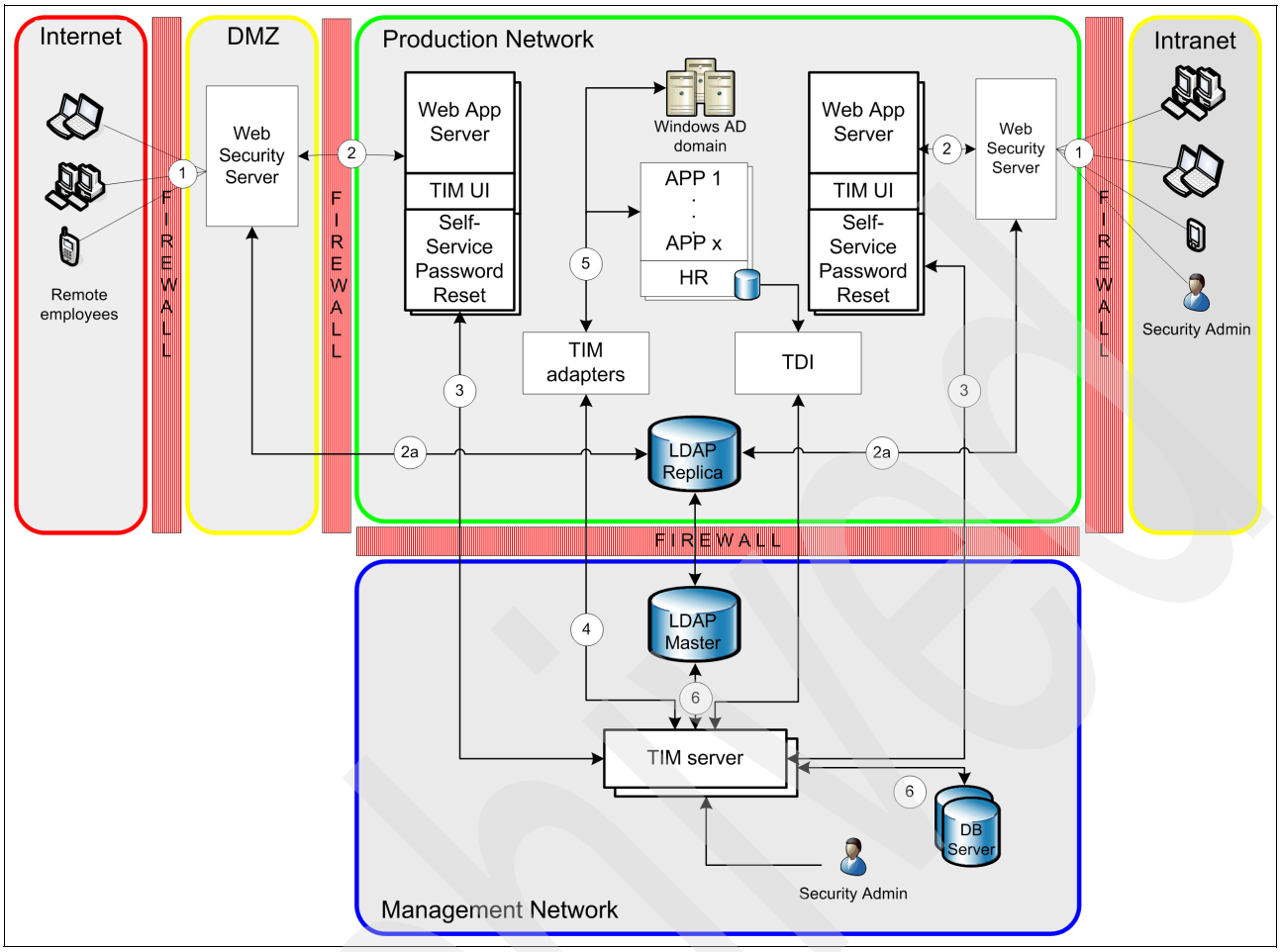

Figure 2-2 Phase 2 implementation architecture

In the second phase, the retailer addresses the following issue:

- Reduce costs for IT help desk and administration, and save employees time by providing the ability to reset the employee password, view account details, and view account access rights.

The account management self-service feature can be configured and managed by using the regular Tivoli Identity Manager administrative web user interface. Because all the account management operations are executed by Tivoli Identity Manager, a centralized audit trail is maintained regardless of whether the account management is being performed by system administrators or by delegated administrators. The self-service feature also enables users to request the creation, modification, and deletion of accounts owned by persons whom they supervise.

The Tivoli Identity Manager self-service feature is simple to implement in an existing Tivoli Identity Manager deployment, and it can result in significant cost savings. The Tivoli Identity Manager self-service feature requires giving Tivoli Identity Manager accounts to all users, educating users about how to set their challenge/response questions and answers, and how to use the password-reset feature.

Data flow

As you read through the following data flow example, refer to Figure 2-2 on page 19:

1. Any user can access the Tivoli Identity Manager self-service UI application through a web browser.
2. All internal and external web-based access is being routed through an existing Web Security Server, which redirects the requests to an application server with the Tivoli Identity Manager self-service UI application installed. Figure 2-2 on page 19 shows 2a:
   a. Upon a user's request to access this application the Web Security Servers will authenticate the users through an LDAP server. Access is allowed only if the user is successfully authenticated and has been granted sufficient access privileges. A single sign-on protocol provide the user's credentials to the Tivoli Identity Manager self-service UI application.
3. The Tivoli Identity Manager self-service UI application communicates with the Tivoli Identity Manager server.

   If the password-reset function is requested, the application presents the challenge/response question (or questions) for the authenticated user. If the correct answers are provided, the password for all Tivoli Identity Manager managed resources updated and distributed.

   If a user requests any new resources or accesses, Tivoli Identity Manager may (after a successful approval workflow, for example) provision a user account for a new managed resource.
4. Any of the requested and approved changes from step 3 are provisioned by Tivoli Identity Manager using the Tivoli Identity Manager adapters. Tivoli Identity Manager checks all existing provisioning policies and authorization policies to evaluate whether the user request can be implemented.
5. A Tivoli Identity Manager adapter eventually communicates with the managed resources to implement the user requests.
6. The provisioning results are logged within the Tivoli Identity Manager database server. The use- relevant information is stored within the LDAP server.

Implementation steps

The password-reset self-service implementation steps are as follows:

To implement the password-reset self-service, perform the following steps:

1. To use the password self-service function, configure the use of challenge/response questions. When this feature is implemented, inform the users about how to set up their challenge answers and how to use the password-reset feature in the self-service application.
2. Enable access to the Tivoli Identity Manager self-service user interface for every user on the web application server. This step may include the definition of access control information for your Web Security Server environment.
3. Enable the account management self-service feature using the administration UI.
4. Configure delegation policies to enable the capability for users to request additional resources and accesses. For this, define roles, policies, and accesses for *specific access rights*, such as the following definitions, for example:
   – User groups in *corporate applications*: All employees must have access to corporate applications only with user rights. And users should be able to request additional accesses based on their permissions and their entitlements.

– Manager groups in *corporate applications*: All users with special access (manager access) must have access to corporate applications and must have manager group membership. This way managers can grant access for a user who is entitled for that application.
– Roles and policies for any *specific system and application access*, for example users from Microsoft Active Directory infrastructure.

5. Set up, for example, a semi-annual or annual review process where first users and then their managers recertify their continuing need for their roles.

2.1.3 Phase 3: Implementing enterprise single sign-on

To provide a homogeneous workplace experience for employees to increase productivity and reduce frustration over a number of distributed kiosk type workstations the retailer begins to implement an enterprise single sign-on solution.

Instead of being prompted to log on to individual applications several times a day (because of timeout and inactivity properties) the employees will be able to access all IT related resources by using their proximity badge on all the distributed Microsoft Windows-based kiosks throughout the retail floor and in individual office environments.

The single sign-on infrastructure manages access profiles for individual applications on a per-user base. These user individual profiles are accessible from a variety of workstations and kiosks throughout the infrastructure.

This solution will also be integrated with the already installed identity life-cycle management solution so that automatically provisioned new resources can be added to or removed from single sign-on access profiles of the users. When an employee leaves the company, the identity life-cycle management solution ensures that all user information is removed from the single sign-on systems also.

In this phase, the password-reset self-service capability also extended to include kiosk and workstation access, a function that had to be performed by administrative personnel before (because the web-based password-reset application is not available when users cannot log in to their workstations).

In the first step of this third phase, the retailer continues to use the regular user ID and password combination for authentication of users. In a second step they will focus on adding proximity badge readers for all kiosks and workstations. The general proximity badge infrastructure is already in place and it is being used for physical access control.

Figure 2-3 on page 22 shows the additional components that are being implemented after the successful Tivoli Identity Manager deployment. The existing components are in place, but the non-essential communication connectors are disabled (grayed out). The Tivoli Access Manager for Enterprise Single Sign-On Integrated Management System server (TAM E-SSO IMS server) and IMS database server are being deployed on individual machines for better scalability. The figure also shows that they are being deployed in a clustered fashion to provide high availability.

More information: For more information about deployment models of Tivoli Access Manager for Enterprise Single Sign-On, see *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350.

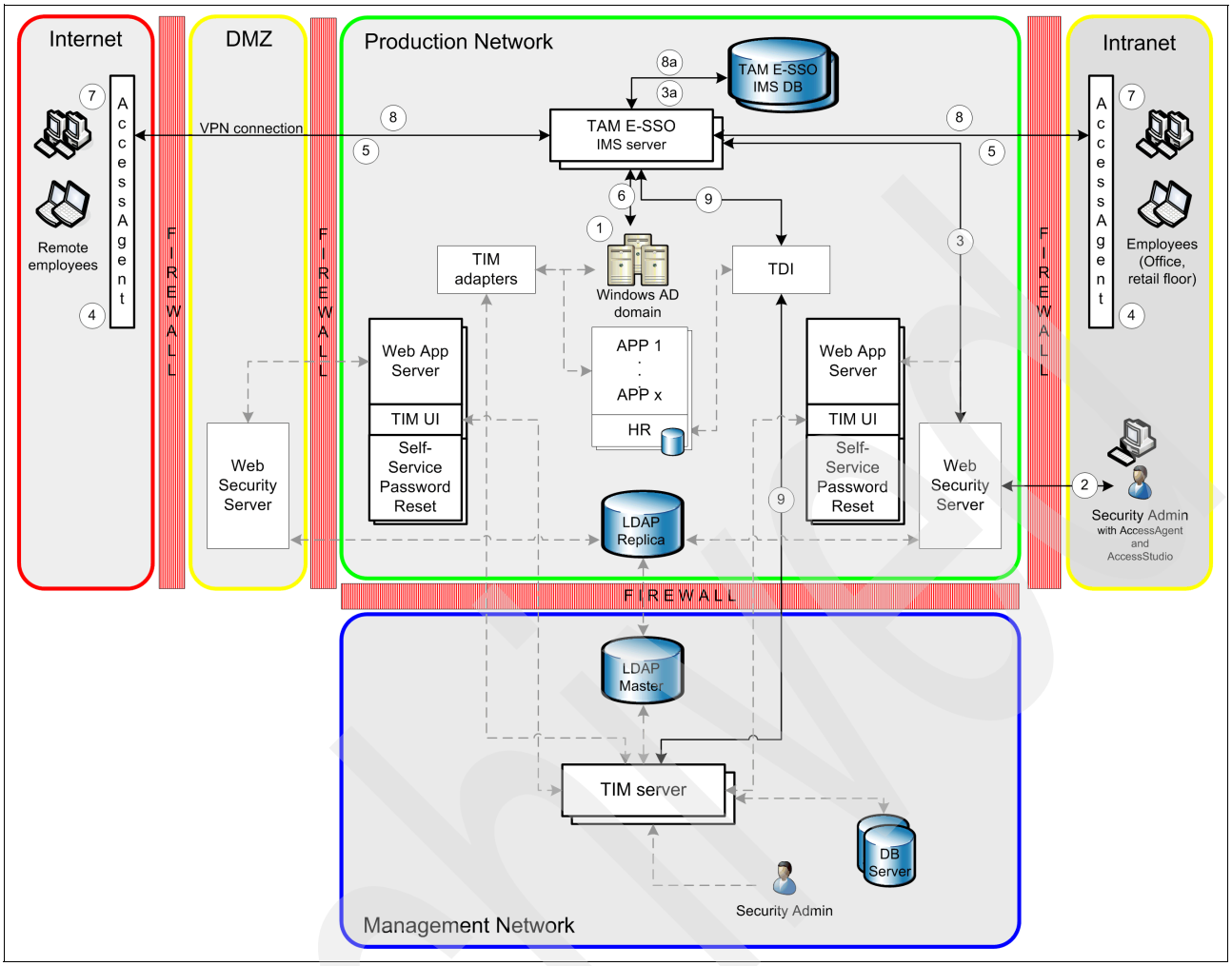

Figure 2-3 Phase 3 implementation architecture

This third phase addresses the following issues:

- Reduce the workload on employees, with respect to password management.
  - Save time and effort required by employees who log in to many various applications over the course of a day.
  - Save time and costs managing Windows desktop password resets.
- Enforce the corporate security policy for all user accounts and their attributes, access rights, and password rules.
- Further reduce the cost of administering users and their accounts.

These goals can be achieved by deploying Tivoli Access Manager for Enterprise Single Sign-On and tying it into the Tivoli Identity Manager infrastructure.

No external use for this project phase: Remember, the retailer is not including single sign-on functionality for customers or any other external party at this time. The deployment architecture diagram in Figure 2-3 on page 22 shows that the remote employees (office staff, management, administration, and so on) are included in the single sign-on project running their Windows-based computers over an Internet connection. The physical network connection that is established from the individual workstations (through the DMZ) into the corporate production network zone must be based on a secured connection like a VPN.

For a successful implementation, the retailer uses the following steps:

1. Perform Base setup and application integration.

   Deploy Tivoli Access Manager for Enterprise Single Sign-On Access Agent to several test systems and deploy the IMS server and IMS database server infrastructure. Create several application profiles for single sign-on integration:

   – Email and collaboration applications using IBM Lotus® Notes®
   – Web based applications using web browser access
   – Custom applications for the retail floor

2. Configure the Tivoli Access Manager for Enterprise Single Sign-On password self-service function to address the password-reset issue by allowing users to reset forgotten desktop passwords for their workstation.
3. Configure the Tivoli Access Manager for Enterprise Single Sign-On shared desktop feature to allow employees to access applications from shared-desktop machines on the retail floor. This step is implemented in a way that multiple users do not have the need for an individual desktop but rather can share one and the same environment. When a user leaves a retail floor workstation, the user is automatically logged off any enterprise application.
4. Integrate Tivoli Identity Manager.

   Enable the existing provisioning system based on Tivoli Identity Manager to provision and manage user accounts in concert with Tivoli Access Manager for Enterprise Single Sign-On.

5. Deploy Tivoli Access Manager for Enterprise Single Sign-On to the employees' office and kiosk systems. At this time, inform the employees about how to interact with the new single sign-on system.
6. As mentioned previously, the retailer will eventually add authentication support for their proximity employee badges by installing RFID readers to all applicable workstations.

Data flow

As you read through the following data flow example, refer to Figure 2-3 on page 22:

1. A working organization directory such as Windows Active Directory already exists and is operating.
2. The administrator configures a database on the IMS database server. The administrator installs the IMS Server software. This step must be done before any AccessAgents are installed.

   If the administrator wants to manage SSO profiles from his or her machine, AccessAgent and AccessStudio software must be installed.

3. With the help of the AccessAdmin web console, the administrator configures the IMS Server with the organization directory for authenticating the user. At this step, the initial AccessProfiles and machine policies are defined. Figure 2-3 on page 22 shows 2a:

   a. All configuration items belonging to the profiles, like AccessProfiles or machine policies, are stored in the IMS database.

4. When the IMS Server is running and the initial profiles are defined, the AccessAgent can be deployed onto the Windows clients.

5. During the installation phase, the AccessAgent registers itself at the IMS Server and downloads the required machine policy.

6. If manual sign-up for new Tivoli Access Manager for Enterprise Single Sign-On users is configured, the user has to authenticate with the organization directory credentials. Usually these are the Active Directory credentials.

   The IMS Server checks the sign-up credentials always against the organization directory that is configured into the IMS Server.

   During the user sign-up, a new Wallet for the user is created, stored in the IMS database, and downloaded to the AccessAgent together with the required UserProfile.

7. From this step forward, the user is operating as usual.

   During normal operations the user authenticates against the locally installed AccessAgent, and no longer against the operating system. If a connection to the IMS server is not available at that time, the authentication process can still take place with locally cached (and encrypted) user profile information that is stored in a *Wallet*. After the user is successfully authenticated against the AccessAgent, the first single sign-on action is to log the user into the local operating system.

8. If a connection is available, the IMS Server verifies the user credentials provided by the user. The AccessAgent then synchronizes any updates from the user wallet back to the local workstation.

   In regular, configurable intervals, the AccessAgent connects to the IMS server to check for further updates and to send audit information from the workstation.

   a. All Tivoli Access Manager for Enterprise Single Sign-On data is being stored within the IMS database (shown as 8a in Figure 2-3 on page 22).

9. In this last step the retailer looks at the Tivoli Identity Manager integration. The retailer uses the Tivoli Identity Manager Adapter for IBM Tivoli Access Manager for Enterprise Single Sign-On, which is located on the Tivoli Directory Integrator server, to automate the following administrative tasks:

   – Create new users on the Tivoli Access Manager for Enterprise Single Sign-On server.
   – Delete user accounts on the Tivoli Access Manager for Enterprise Single Sign-On server.
   – Reconcile users on the Tivoli Access Manager for Enterprise Single Sign-On server.
   – Add and change a password, delete credentials in the user's Tivoli Access Manager for Enterprise Single Sign-On Wallet.

When any of the previously mentioned administrative actions occur (either manually or automatically), Tivoli Identity Manager sends the request to Tivoli Access Manager for Enterprise Single Sign-On by using the adapter that is deployed on the Tivoli Directory Integrator server.

Implementation steps

The enterprise single sign-on implementation steps are as follows:

1. Because an enterprise directory (based on Windows AD) already exists, the administrator starts the implementation by configuring a database on the IMS database server. The administrator then installs the IMS Server software, which must be done before any AccessAgents are installed. If the administrator wants to manage SSO profiles from the administrator's machine, the AccessAgent and AccessStudio software must be installed.
2. With the help of the AccessAdmin web console, the administrator configures the IMS Server to connect to the organization directory for initially authenticating the user. In this step, the initial AccessProfiles and machine policies are defined also.
3. When the IMS Server is running and the initial profiles are defined, the AccessAgent can be deployed onto the Windows clients.
4. During the installation phase, the AccessAgent registers itself at the IMS Server and downloads the required machine policy.
5. If manual sign-up for new Tivoli Access Manager for Enterprise Single Sign-On users is configured, the user has to authenticate with the organization directory credentials. Usually these are the AD credentials.
6. The IMS Server checks the sign-up credentials always against the organization directory that is configured at the IMS Server.
7. During the user sign-up a new wallet (which holds the user credentials that are required for single sign-on) for the user is created, stored in the IMS database, and downloaded to the AccessAgent together with the required UserProfile.

More information: For more details about how to plan, design, and implement Tivoli Access Manager for Enterprise Single Sign-On, see *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350.

For the integration with Tivoli Identity Manager, the administrator has to install the Tivoli Access Manager for Enterprise Single Sign-On provisioning bridge and workflow extensions, which are the interface engines that act as intermediaries between the IMS Server and Tivoli Identity Manager. The main implementation steps are as follows:

1. Install and configure the Tivoli Access Manager for Enterprise Single Sign-On adapter (partly on Tivoli Directory Integrator and Tivoli Identity Manager servers).
2. Configure the IMS Server.
3. Configure the workflow extensions on Tivoli Identity Manager.

More information: For more details about this implementation, see "Chapter 9 - Tivoli Identity Manager implementation" in *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350.

Now, the single sign-on infrastructure is operational. The users are able to access their applications immediately after authenticating to the Windows workstation by using AccessAgent, initially with a user ID and password combination, and later by using their retailer's proximity badge.

2.2 Log and access management for audit readiness

In this scenario, a large financial institution wants to address the following requirements:

- Reduce escalating operational costs for access and audit log management.

  The financial institution is subject to SOX[2], GLBA[3], and other government and internal rules and regulations. As these rules and regulations change, log retention requirements, log details, and actions that require logging change also.

  A centralized approach is required to manage log collection, retention, and reporting. The log data must be easily accessible for forensic activities and to provide compliance reports during audits.

- Reduce escalating operational costs for user access and data management because of an increasing number of applications in the IT environment and because of an elevated change in the user population.

  The financial institution has to constantly maintain account types, access to internal employee applications and application data. The IT staff is required to update access control lists for many applications when an employee's responsibilities change.

- Provide a single interface to manage user and data access to ensure access rights are granted uniformly.

  Because of the large number of applications in the financial institution, the IT staff has to manually update access control lists on separate applications. Occasionally, access is not removed for an employee when that employee no longer needs access, and sometimes access is not granted for an application that the employee should receive. These issues can lead to problems when the organization is being audited for compliance and can lead to lost productivity for employees.

  A centralized access management environment is needed to address the increasing operational costs and audit risks posed by ad-hoc access management.

To address these requirements, the financial institution has decided to implement the project in two phases:

- Phase 1: Implementing improved log management
- Phase 2: Implementing improved access controls for applications

2.2.1 Phase 1: Implementing improved log management

To improve log retention and standardize log management, the financial institution chose to implement centralized log management and compliance reporting by using IBM Tivoli Security Information and Event Manager. Figure 2-4 on page 28 introduces the following services (in the figure, TSIEM is the Tivoli Security Information and Event Manager):

- A Tivoli Security Information and Event Manager *cluster configuration* is deployed in the Management Network zone. It consists of one Enterprise Server and one or more Standard Servers:
  - The Tivoli Security Information and Event Manager *Enterprise Server* is a Windows- or UNIX-based server that provides centralized log management and forensic functions, allowing these features to operate across multiple Tivoli Security Information and Event Manager Standard Servers. As shown in Figure 2-4 on page 28, the Enterprise Server can offer consolidated log management facilities over all connected Tivoli Security Information and Event Manager Standard Servers. From one

[2] Sarbanes-Oxley Act (SOX): http://www.sarbanes-oxley.com/
[3] Gramm-Leach Bliley Act (GLBA): http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

Enterprise Server you can get a consolidated view of log collections and log collection continuity, which simplifies the management of a Tivoli Security Information and Event Manager cluster. It can reduce your operational overhead, and provide a single view for auditors to examine the complete log history.

– Tivoli Security Information and Event Manager uses a centralized Windows-based server, called the *Standard Server*, as the heart of its security audit and compliance system. The Standard Server performs the following main functions:

  - Collects security logs from audited event sources.
  - Archives the logs.
  - Normalizes the event data and loads it into the reporting databases.
  - Sends email alerts when a high severity event is detected.
  - Creates reports.

► The events found in the logs are normalized and stored in databases. The data in the databases is available for further investigation through a web-based tool called the *Compliance Dashboard*. The Compliance Dashboard is a reporting application that Tivoli Security Information and Event Manager administrators can use to generate specific reports on compliance level and policy violations. It uses an HTTP server, authorizing users to view reports through their web browser.

► Another main component of the Tivoli Security Information and Event Manager system is the *Management Console*, which is used to manage and configure the system. Each Standard Server has its own configuration database managed by the Management Console.

The Management Console can operate locally or in a distributed manner, as shown in our example. All that is required for remote operation apart from the Management Console itself is a local Tivoli Security Information and Event Manager *Agent* through which it can communicate. In our deployment, the financial institution has decided to have the Security Administrators communicate with a Management Console in the Production Network and keep the restricted communication into the Management Network open only for direct traffic from agent to Tivoli Security Information and Event Manager Server.

► *Collection* is the process of centralizing event data by retrieving it from the audited machines and applications and archiving it in the *Log Management Depot*, the central storage repository for log data on the Tivoli Security Information and Event Manager server. To exchange information between its components, Tivoli Security Information and Event Manager uses a virtual private network consisting of *Agents* that maintain encrypted communication channels.

This network runs on the TCP/IP layer of the existing organizational network. The two methods of data collection are as follows:

– Locally installed software (Agent) on the target machine, as shown for the Linux Application and Database Servers

– Agentless collection, which can be achieved by either of the following methods:

  - A remote Agent installation that allows you to collect the application security log that is located on a separate host machine, as shown for Active Directory (AD), and File and Print Server, the Linux Web Servers, and the Windows 2003 Swift Connector
  - The Tivoli Security Information and Event Manager server acting as a point of presence to collect the data

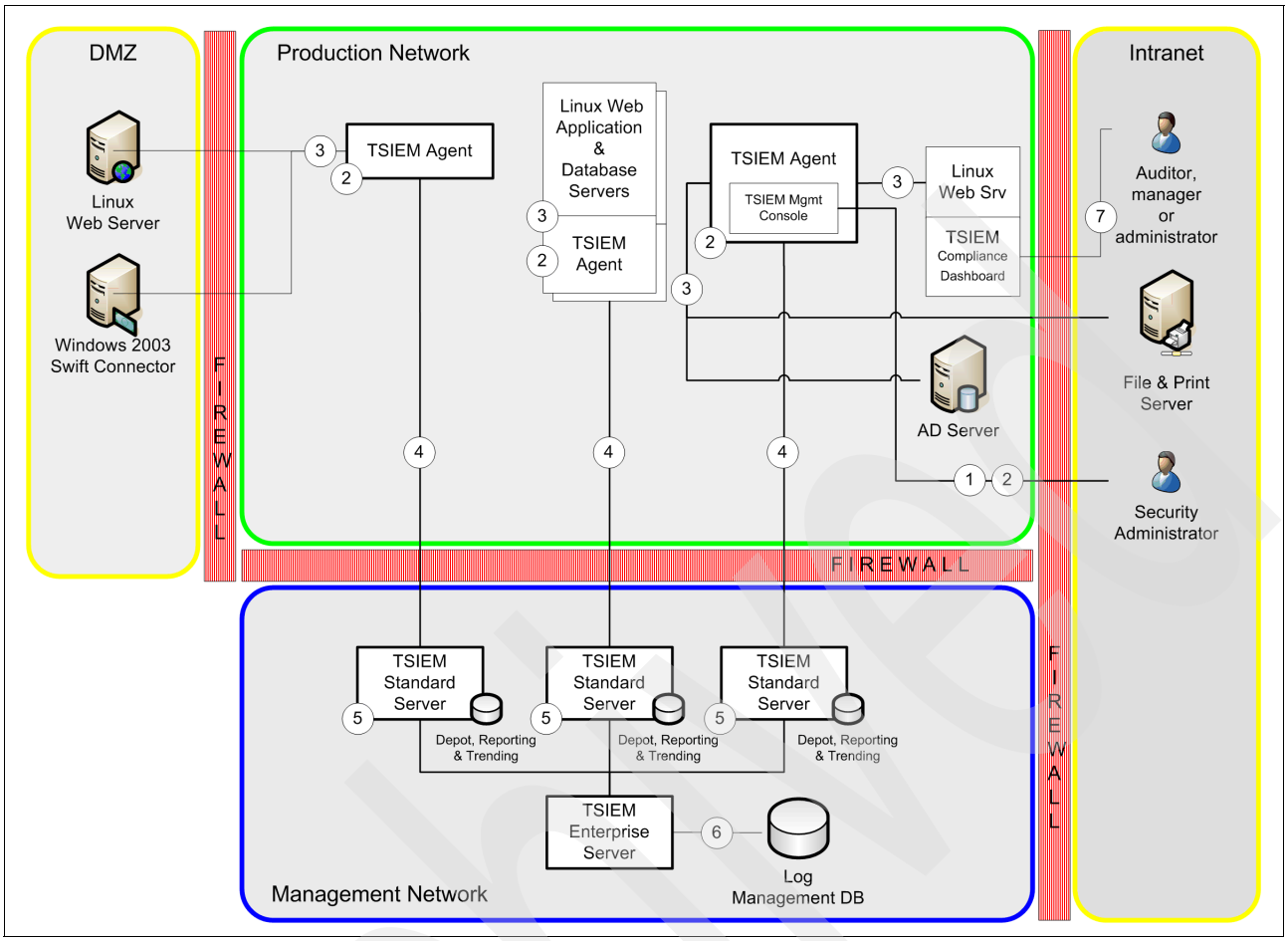

Figure 2-4 Phase 1 implementation architecture

More information: See the following resources for more information about Tivoli Security Information and Event Manager components:

- *IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager*, SG24-7530
- IBM Tivoli Security Information and Event Manager Information Center:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tsiem.doc/welcome.html

With Tivoli Security Information and Event Manager, the financial institution can address the following issues :

- The institution monitors privileged users and their activities on key corporate systems and data to ensure that confidentiality, integrity, and the availability of systems is properly maintained. The monitoring and auditing can help prevent costly damages or outages because of inadvertent mistakes or malicious actions of privileged users.
- The institution centralizes its logging by using automatic, fast, reliable log file collection and management throughout the distributed IT environment, including various applications, operating systems, and databases. The centralized logging mechanism is configurable so it can change as corporate requirements and reporting needs evolve.

Historical log data is accessible to get a global view of the organization's compliance posture.

> **More information:** For information about security compliance standards, see *IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager*, SG24-7530.

For a successful implementation, the financial institution follows four steps:

1. Analyze and evaluate reporting requirements, discover and learn about the implementation environment, and define audit settings that support reporting requirements for all event sources on platforms that need to be monitored.
2. Define and plan the project. With acquired base information, implement a pre-planning worksheet, based on target platforms (with server and application names, platforms and versions, daily log sizes, server location, database groupings, and so on). Then, define a draft project plan with an initial project schedule, reporting requirements, and installation environment information. The plan has to be based on a typical Tivoli Security Information and Event Manager implementation design architecture (number and location of Tivoli Security Information and Event Manager servers, hardware specifications, and so on) and installation prerequisites (software and platform versions, audit settings, ports, and so on).
3. Verify that the recommended audit settings are in place and that all systems are configured as suggested in the prerequisites (Tivoli Security Information and Event Manager servers hardware, audit settings, TCP/IP connectivity, and so on). Then, begin the implementation.
4. Monitor and adjust the policy exceptions for improvement. Report and translate the effectiveness of the controls compared to the security objectives. Adjust policies and reporting constantly to reflect changes in the organization. Tune policies to eliminate normal events. Modify groups on an as-needed basis and document all changes and settings.

Data flow

As you read through the following data flow, refer to Figure 2-4 on page 28.

1. The Security Administrator uses the Management Console to configure and manage the Enterprise Server and the individual Standard Servers, including collection schedules. The Management Console can operate locally or in a distributed manner and can be placed anywhere in the network as shown in our scenario. A prerequisite for remote operation apart from the Management Console itself is a local Agent, which is used for console-to-server communication.
2. The *collection schedules* are triggered automatically based on configured settings. Alternatively, a manual collection command can be given to a Tivoli Security Information and Event Manager server by a Security Administrator using the Management Console. A Tivoli Security Information and Event Manager server issues an *audit trail collect* command to the Agent. This command activates the Agent on the audited machine.
3. The appropriate Agent script reads the security log and collects only those new records since the last collection.

Additional configuration options: The actual collection process can involve various mechanisms in a variety of configurations. A system audited through remote collect does not need to run the Tivoli Security Information and Event Manager software. Instead, event data is forwarded to the server by a system with an Agent with direct access to the audited system. For more information about Tivoli Security Information and Event Manager concepts and various configurations, see the *IBM Tivoli Compliance Insight Manager User Guide Version 8.5*, SC23-6581.

4. In a *collection* process, the Agent formats the log records into a *chunk* format and compresses the chunks. A chunk can contain many log types from the audited machine. The Agent reads the chunk log data and it securely sends the chunk data in encrypted form to the Agent on the Tivoli Security Information and Event Manager server.

   After successfully sending the chunks to the Tivoli Security Information and Event Manager server, the Agent deletes its local copy of the chunk. Additionally, on certain platforms, the Agent is setup to delete the original audit trail, if appropriate.

5. When the chunks are received, a Tivoli Security Information and Event Manager server runs several automated processes. Together, these processes provide a complete solution from collecting and analyzing logs to reporting and auditing activities for compliance.

   First, the retrieved event data is stored on the Standard Server in the Log Management Depot. For analysis, the data is taken from the Log Management Depot and normalized into a W7 data model called *General Event Model* (GEM). This process is called *mapping*. Subsequently, the mapped data is loaded into the Reporting Database.

   Each W7 event record includes the following information:

   Who Which user or application initiated the event?

   What What kind of action does the event represent?

   When When did the event occur?

   Where On which machine did the event happen?

   OnWhat What was the object (file, database, printer) involved?

   WhereFrom From which machine did the event originate?

   WhereTo Which machine is the target or destination of the event?

   Data and statistics, spanning a longer period, are maintained by a process called *aggregation*. The aggregation process builds a special database, called the Trending Database, from which trends and summaries can be extracted.

6. For enterprise-wide trending and forensics in a Tivoli Security Information and Event Manager cluster environment, Trending Databases from multiple Standard Servers are brought together into a single consolidation database on the Enterprise Server.

7. Tivoli Security Information and Event Manager's web-based reporting tool, the *Compliance Dashboard*, provides a large number of standard and custom reports. These reports are produced on request by the Compliance Dashboard, which pulls information from mapped data, including that stored in the Trending Database. These reports can highlight attempts to breach security and (attempted) access to critical resources.

   You may use both standard and custom reports to examine exceptions and events that require special attention, and because the data presented in these reports is in the W7 format, no specialized knowledge is required to interpret the output. Reports are clear, concise, and integrate all security data for your review.

   Tivoli Security Information and Event Manager Compliance Dashboard also provides a dashboard with graphical and statistical overviews of logged activities, with drill-down

capabilities to identify and examine related events. Additionally, Tivoli Security Information and Event Manager's illustration of policy exceptions enables you to continuously monitor and tailor your security policies to your changing business needs.

More information: See the following resources for product architecture and processes:

- *IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager*, SG24-7530
- *IBM Tivoli Compliance Insight Manager User Guide Version 8.5*, SC23-6581

Implementation steps

The automatic provisioning service implementation steps are as follows:

1. Install Tivoli Security Information and Event Manager Standard and Enterprise Servers.
2. Install necessary Agents per platform type.
3. Activate the event sources.
4. Activate auditing for all event sources.
5. Collect and load the data.
6. Build the W7 model, policy, and rules.
7. Configure the alerts.
8. Create and code the reports.
9. Configure report distribution.

2.2.2 Phase 2: Implementing improved access controls for applications

To streamline access control and audit logging on existing UNIX servers and web applications, the financial institution chose to implement a centrally managed access control solution using IBM Tivoli Access Manager for Operating Systems (TAMOS) and IBM Tivoli Access Manager for e-business (TAMeb).

To make the centralized access management implementation as effective as possible, the financial institution now hosts all of their web based applications on the Linux Web Application Servers that are located in the Production Network zone. Access to those applications will only be granted by passing through reverse proxy engines that verify access credentials based on individual user priveleges. For example, this includes moving the Tivoli Security Information and Event Manager Compliance Dashboard to this server.

Figure 2-5 on page 34 introduces the access management services.

Tivoli Access Manager's base functions are provided through a set of core components and various management components. The two core components are a *user registry* and an *authorization service* consisting of an *authorization database* and an *authorization engine*.

These components support the core functionality that must exist for Access Manager to perform its fundamental operations, which are as follows:

- Knowing the identity of who is performing a particular operation (users)
- Knowing the roles associated with a particular identity (groups)
- Knowing what application entities a particular identity may access (objects)
- Knowing the authorization rules associated with application objects (policies)
- Using this information to make access decisions on behalf of applications (authorization)
- Auditing and logging all activity related to authentication and authorization

In summary, a user registry and an authorization service are the fundamental building blocks upon which Tivoli Access Manager builds to provide its security capabilities. All other services and components are built on this base.

The central management component to maintain the the authorization database and the user registry is the *Policy Server*. This component is typically deployed within a restricted Management Network zone, because you want to reduce its exposure as much as possible. Note the following information:

- The authorization database contains object definitions that may represent logical or actual physical resources. These definitions are referred to as the *protected object space*, and they contain the following security mechanisms:
  - Access control list (ACL) policy templates
  - Protected object policy (POP) templates
  - Extended attributes
  - Authorization rules

  The Tivoli Access Manager authorization service uses the protected object space to make its access control decisions. Because a typical Tivoli Access Manager deployment can consist of many distributed authorization services (often referred to as a *resource manager*), the master authorization database is being replicated to the appropriate authorization services, for example the Tivoli Access Manager WebSEAL and Tivoli Access Manager for Operating Systems (TAMOS) resource managers, shown in Figure 2-5 on page 34.

  The authorization database is always encrypted when stored on a disk or when in transfer to distributed authorization services.
- Tivoli Access Manager requires a user registry to support the operation of its authorization functions. Specifically, it provides the following items:
  - A database of the user identities that are known to Access Manager.
  - A representation of groups in Access Manager that may be associated with users.
  - A data store of other metadata required to support authorization functions.

  Tivoli Access Manager supports many types of user registry products. In this scenario, the registry is called an LDAP user registry.

  The LDAP master, in this case, is deployed in the Management Network. It is the only LDAP component that receives updates. Also, the scenario is deploying two separate LDAP replicas that will be queried by the distributed authorization services. The decision was to use two LDAP replicas to better balance load between internal and external web traffic.

The two major Tivoli Access Manager management facilities in this deployment are as follows:

- The *pdadmin utility*, which provides a command-line capability for performing administrative functions such as adding users or groups,
- The *Web Portal Manager*, which provides a web browser-based capability for performing most of the same functions provided by the pdadmin utility.

To enforce the centrally managed access control policies, the scenario deploys two resource managers, which are the Tivoli Access Manager for Operating Systems and theTivoli Access Manager for e-business WebSEAL component:

- Tivoli Access Manager for Operating Systems is being deployed on key UNIX and Linux systems because these systems have an inherent weakness in producing useful audit information and ensuring compliance with corporate security policy.

  Tivoli Access Manager for Operating Systems provides a layer of authorization policy enforcement in addition to that provided by a native UNIX operating system. It can apply fine-grained access controls that restrict or permit access to key system resources. Controls are based on user identity, group membership, the type of operation, time of the day or day of the week, and the accessing application. An administrator can control access to specific file resources, login and network services, and changes of identity. These controls can also be used to manage the execution of administrative procedures and to limit administrative capabilities on a per-user basis. In addition to authorization policy enforcement, mechanisms are provided to verify defined policy and audit authorization decisions.

  Access control information is stored in the authorization database that is centrally maintained by the Policy Server. The accessing user definitions are stored in a user registry that is also centrally maintained in the environment. When protected resources are accessed, Tivoli Access Manager for Operating Systems performs an authorization check based on the accessing user's identity, the action, and the resource's access controls to determine whether access should be permitted or denied.

  In addition, Tivoli Access Manager for Operating Systems can control access to specific file resources, login and network services, and changes of identity. These controls can also be used to manage the execution of administrative procedures and to limit administrative capabilities on a per-user basis. In addition to authorization policy enforcement, mechanisms are provided to verify defined policy and audit authorization decisions.

- Tivoli Access Manager for e-business WebSEAL is a high-performance, multi-threaded reverse proxy, that is deployed in front of back-end web servers. It can apply a security policy to the protected object space (which is defined in the authorization database). WebSEAL can provide single sign-on solutions and incorporate back-end web application server resources into its security policy. Being implemented on an HTTP server foundation, it listens to the typical HTTP and HTTPS ports. WebSEAL can handle connections to secured and unsecured web resources.

  WebSEAL is typicaly being deployed in the Internet DMZ to act as an HTTP/HTTPS gateway into the organization. When protecting web-based resources towards the organization's intranet users, it is typically located in the Production Network zone. After a WebSEAL infrastructure is in place, you want to make sure that all HTTP/HTTPS traffic that reaches your web applications and resources is originating from a WebSEAL server. No other traffic is allowed.

More information: See the following resources:

- *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014
- Tivoli Access Manager for e-business Information Center:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.itame.doc/toc.xml

- Tivoli Access Manager for Operating Systems Information Center:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamos.doc/welcome.htm

The Tivoli Security Information and Event Manager infrastructure, which has already been deployed in Phase 1 (described in 2.2.1, “Phase 1: Implementing improved log management” on page 26) can now be configured to work with the additional Tivoli Access Manager audit log information provided by the WebSEAL and Tivoli Access Manager for Operating Systems components.

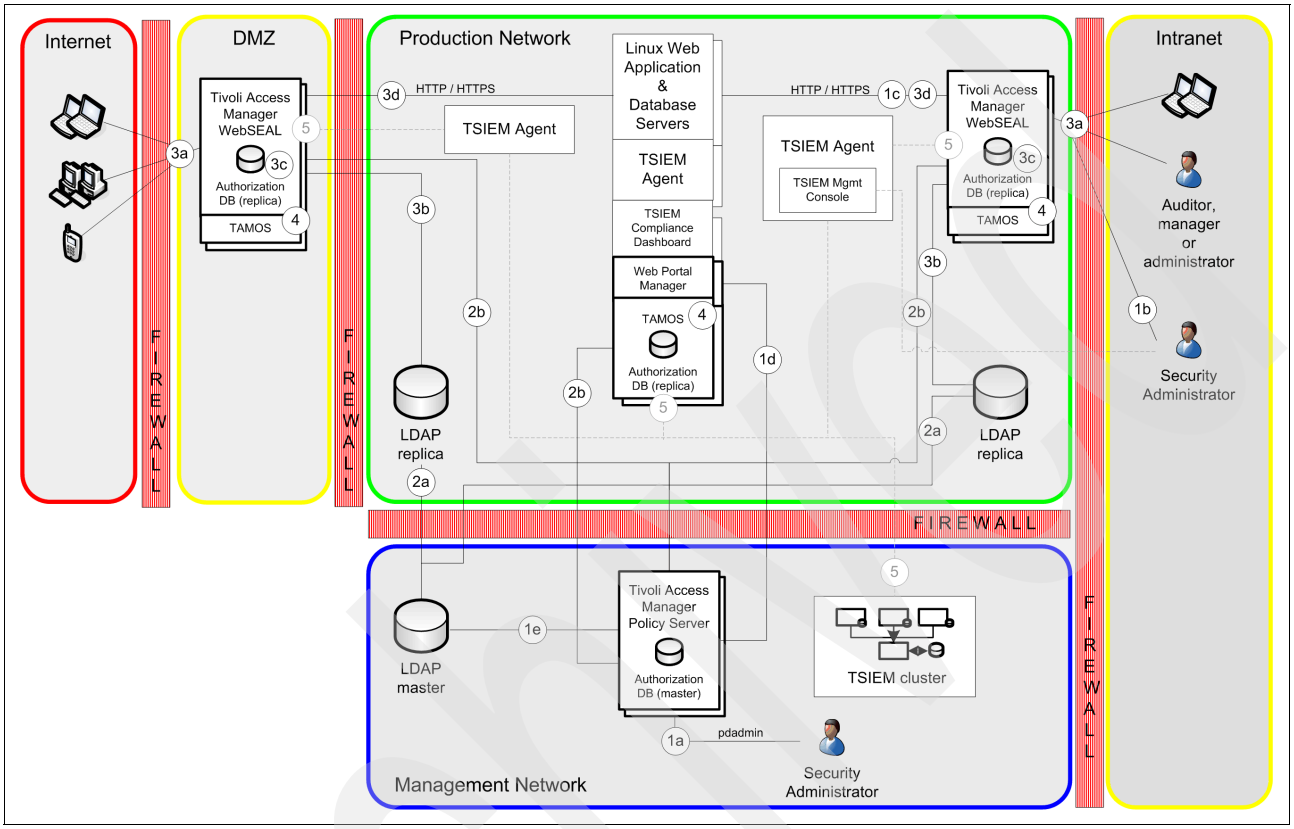

Figure 2-5 Phase 2 implementation architecture

With this deployment, the financial institution mitigates security risks that currently exist in their UNIX and Linux environment and provide the required level of logging detail. To be compliant with internal and external security requirements, the audit trail now indicates the individual user performing privileged operations. Besides addressing logging and compliance, the financial institution now centrally manage all its access control policies for web applications. There no longer is a need to manage user access information for applications separately.

With Tivoli Access Manager for Operating Systems and Tivoli Access Manager for e-business, the financial institution addressed or implemented the following items:

- Single policy enforcement engine for web application access control
- Single view for UNIX and Linux security access policy
- Auditable privileged user activity to comply with internal and external regulations
- Improved access control to web applications and content at the URL level, which may be hosted on multiple web servers
- Centralized auditing for all attempts to access corporate resources to determine if systems are secure, which is important for audit readiness and compliance with regulations such as Sarbanes-Oxley
- Fine-grained authorization capability within distributed applications

- Consistent application security policy throughout the business, which saves business resources by removing multiple, competing security infrastructures
- Consolidation of detailed audit data provided by Tivoli Access Manager for Operating Systems and Tivoli Access Manager for e-business into Tivoli Security Information and Event Manager.

Data flow

As you read through the following data flow, refer to Figure 2-5 on page 34:

1. All policies related to Tivoli Access Manager (ACLs, protected object policies, and extended attributes) are centrally managed and stored in the Tivoli Access Manager master authorization database on the Policy Server.
   a. A security administrator may use the **pdadmin** command-line tool. For this access, the administrator must have a connection to the Policy Server that sits within the Management Network zone. (You may either allow this type of administrative access through the firewall or require an administrator to be physically located within this network zone.)
   b. A security administrator can also use the web-based administrative interface, the Web Portal Manager (WPM). WPM has to be deployed on a web application server that is accessible to the administrator.
   c. Because the improved access control policy of the financial institution requires all web-based application accesses to be channeled through the Tivoli Access Manager WebSEAL component for authentication and authorization, the organization has deployed WPM on their central web application server cluster. An administrator authenticates with WebSEAL and then is granted access to WPM.
   d. The firewall into the Management Network zone grants access for specific Tivoli Access Manager administrative ports, so that WPM commands can be executed on the Policy Server.
   e. User- and group-related administrative tasks are being stored in the LDAP master repository that is also deployed in the Management Network zone.
2. Tivoli Access Manager and LDAP can automatically distribute and replicate the information that is stored in the central master databases. This is done to bring the access control decision information as close to the policy decision and enforcement points as possible to reduce network traffic and latency. Note the following information:
   a. LDAP uses its LDAP replication protocol to distribute its data to read-only LDAP replicas. The LDAP replicas that are deployed in the Production Network zone are being used to authenticate users when they are challenged by WebSEAL. WebSEAL submits the user ID and password for the LDAP replica to verify if this combination is legit or not.
   b. The Tivoli Access Manager Policy Server uses its own proprietary protocol to securely replicate its master authorization database to all Tivoli Access Manager related policy enforcement points, in our example, WebSEAL and Tivoli Access Manager for Operating Systems components in the Production Network zone and the DMZ.
3. This step examines how web-based user access is controlled:
   a. When users want to access a web-based resource that is hosted on the organization's central web application server, they must pass through Tivoli Access Manager WebSEAL. If WebSEAL determines that the requested resource is not protected, it grants the users access to that particular resource. When WebSEAL realizes that the users want to access a restricted resource, the authentication and authorization processes start.

b. First, WebSEAL sends the user identity (for example, user ID and password) to the LDAP replica for verification. If LDAP determines that the credentials are not valid, WebSEAL denies access to the resource. If WebSEAL receives a positive answer from LDAP it continues to verify if the authenticated user has the necessary rights to access the resource.

c. Using the user's credentials and the resource information, WebSEAL examines its locally stored authorization database replica to determine whether the user can be granted access to the resource. If the presented credentials do not allow a particular user access to a resource, WebSEAL denies it. If WebSEAL has verified that a user has all necessary access rights in place, it grants access to the hosted web resource.

d. Access to the web resource is granted only after WebSEAL has verified the user's credentials and the applicable access control information for that particular resource.

4. This step examines the Linux-based user access and auditing.

   If a user logs in to any Linux machine with Tivoli Access Manager for Operating Systems installed, the Tivoli Access Manager for Operating Systems security layer authenticates the user and checks for proper authorizations in the local replica authorization database. If the user passes those access control checks, the resource access attempts are turned over to the regular Linux subsystems for standard Linux security evaluation and execution.

   In addition, Tivoli Access Manager for Operating Systems can control and audit the use of application and system components that are part of a *trusted computing base*, prevent the use of compromised resources, and alert the administrators that a security breach has occured.

   Tivoli Access Manager for Operating Systems extends the standard syslog-based Linux auditing. It collects audit information that can be linked back to the originating user, even if, for example, that particular user used the `sudo` command to perform actions under another user ID with separate access rights. All other Tivoli Access Manager for Operating Systems security policy enforcements generate extensive audit trail information that can help eliminate the anonymity of certain privileged user actions.

5. The Tivoli Security Information and Event Manager infrastructure that has been deployed in the previous project phase can now collect the combined logs and audit information from the Tivoli Access Manager for e-business components, Tivoli Access Manager for Operating Systems components, and Linux syslogs to analyze consistent audit trails from these servers and applications. All logs that are collected by the Tivoli Security Information and Event Manager actuators are stored in the Tivoli Security Information and Event Manager cluster in the Management Network zone for future audit or compliance reports.

Implementation steps

The improved access controls across applications implementation steps are as follows:

1. Create and document a Tivoli Access Manager security policy defining the following details:
   - Resources that are hosted on the web application servers, and how those resources are distributed within the organizations network and server infrastructure
   - Custom application resources that must be secured using the Tivoli Access Manager authorization API
   - Roles and groups for the user population
   - Access control lists, protected object policies, and extended attributes
   - Audit and log file collection guidelines and integration with the existing Tivoli Security Information and Event Manager infrastructure

2. Install and configure the following Tivoli Access Manager components:
   - A central Policy Server with stand-by Policy Server (for backup and availability purposes)
   - WebSEAL resource manager clusters in the DMZ and the Production Network zone
   - A master LDAP server in the Management Network zone and replica LDAP servers in the Production Network zone

     If those servers already exist, be sure that applicable Tivoli Access Manager configurations are being performed.
   - Tivoli Access Manager for Operating Systems components on each UNIX or Linux server that will be managed as part of the security policy
3. Create or import users and groups that will access protected resources.
4. Configure WebSEAL junctions and integrations to the protected resources.
5. Attach protected object policies and access control lists to respective groups/resources.
6. Configure the Tivoli Access Manager audit levels as described in the security policy.
7. Create a separate Tivoli Access Manager domain for strict use by Tivoli Access Manager for Operating Systems. This ensures that security policies for the web environment remain separate from the security policies of the UNIX/Linux environment.
8. Define what branches in the protected object space (including POPs and ACLs) have to be created for specific resources.
9. Configure the Tivoli Security Information and Event Manager servers and Tivoli Security Information and Event Manager Agents to properly retrieve and analyze the raw Tivoli Access Manager audit data and map those records into the Tivoli Security Information and Event Manager W7 reporting format.

More information: See the following resources:

- *Deployment Guide Series: IBM Tivoli Access Manager for e-business V6.0*, SG24-7207
- *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014
- *Auditing UNIX/Linux System Use with Tivoli Access Manager for Operating Systems and Tivoli Compliance Insight Manager*, REDP-4402

2.3 Accessing services from external business partners

In this scenario, a healthcare provider wants to access IT services made available by external business partners in a secure manner. The provider wants to increase the available information through the provider's investment in an *enterprise portal* and also improve the user value of the solution. However, the healthcare provider is concerned with the ability to *securely* exchange patient healthcare information with the business partners because of concerns about *sensitivity of data* and *regulatory requirements*. The healthcare provider can mitigate these concerns by establishing the legal, business, and technical trust relationship with its business partners by using web service security and federated identity management standards, and by implementing an enterprise audit and reporting solution. The healthcare provider can also streamline its operations by eliminating the need to maintain and synchronize user authentication credentials (for example, passwords) with each business partner organization. In addition to the operational business benefits, the user experience can be significantly improved, based on the value derived from the additional information available

on the enterprise portal and the elimination of multiple authentication events, one for each provider. Ultimately, the organizations' employees will have access to more information, allowing them to securely provide better business services to customers.

On the business partner side, which in this case is the service provider, there are also several benefits to participating in the trust relationship. The service provider no longer needs to maintain and synchronize user authentication credentials with the healthcare provider. In Phase 1 of this scenario, no additional IT infrastructure is required on the business partner side because the healthcare provider is asserting a user credential that can be consumed by the business partner based on the pre-established *trust agreement*. In Phase 2, the business partner requires a technology solution to support federation protocols, such as *federated identity management*. However, by using a standards-based approach, the business partner is not tied to a particular vendor product.

In this scenario, the healthcare provider wants to address the following requirements:

- Reduce anticipated operational costs for user management and data exchange. Instead of relying on administrative staff to transfer sensitive patient information by mail, fax, or telephone with business partners (such as labs, private practice physicians, or insurance providers), the healthcare provider can enable direct access to data maintained by the provider's business partner ecosystem for doctors and support staff. A federated identity management system is used to securely exchange user credentials between IT solutions of the healthcare provider and business partners.
- Extend business services offered to internal users and external partners. By securely propagating identities for web services and web application transactions, the organization is able to increase the useful information that is available to its users while still making appropriate authorization decisions and capturing audit log information for fully traceable transactions.
- Improve the user experience by increasing the range of services available without requiring additional authentication actions by the user. Through the use of web services security management and federated identity management, the user identity can be securely propagated to web application and web service providers eliminating duplicate authentication requirements.
- Provide a centralized access and audit log management solution to ensure users only access data they are entitled to view. The healthcare provider is subject to HIPAA regulation in addition to other government and internal rules and regulations. The audit solution must ensure that the organization is properly positioned to capture and report on their compliance posture, even as the rules and regulations change over time.

To address these requirements, the healthcare provider has decided to implement the project in the following phases:

- Phase 1: Enabling access to third-party business services
- Phase 2: Enabling federated identity-management-based access
- Phase 3: Implementing centralized logging and reporting

2.3.1 Phase 1: Enabling access to third-party business services

Through the use of Tivoli Federated Identity Manager *web service security management* capabilities, the healthcare provider is able to increase the range of services that are available to its users, including internal and external business partner web-service resources, as shown in Figure 2-6 on page 39 (in the figure, TFIM is Tivoli Federated Identity Manager).

Web service security management provides the ability to exchange user credentials by using a format that is accepted by a service provider. It also offers the ability to create a robust credential containing additional information (for example, user or session relevant attributes). The enrichment of the credential allows the service provider to make authorization decisions based on their policies and provide the proper information in the service response. This model of *requestor makes right* allows the requesting organization to create credentials that are readily accepted by the service provider without placing technical requirements on the service provider to perform a credential exchange process. This model can widely increase the range of services available in the enterprise portal in a secure manner that can be traced to the individual requestor.

In the first phase, the healthcare provider wants to display patient information maintained by multiple service providers, including lab results and patient history information, in the enterprise portal application that is accessed by the medical providers. Tivoli Federated Identity Manager provides the ability to exchange the user credential used by the medical provider at the enterprise portal for a credential type that is accepted by the service provider.

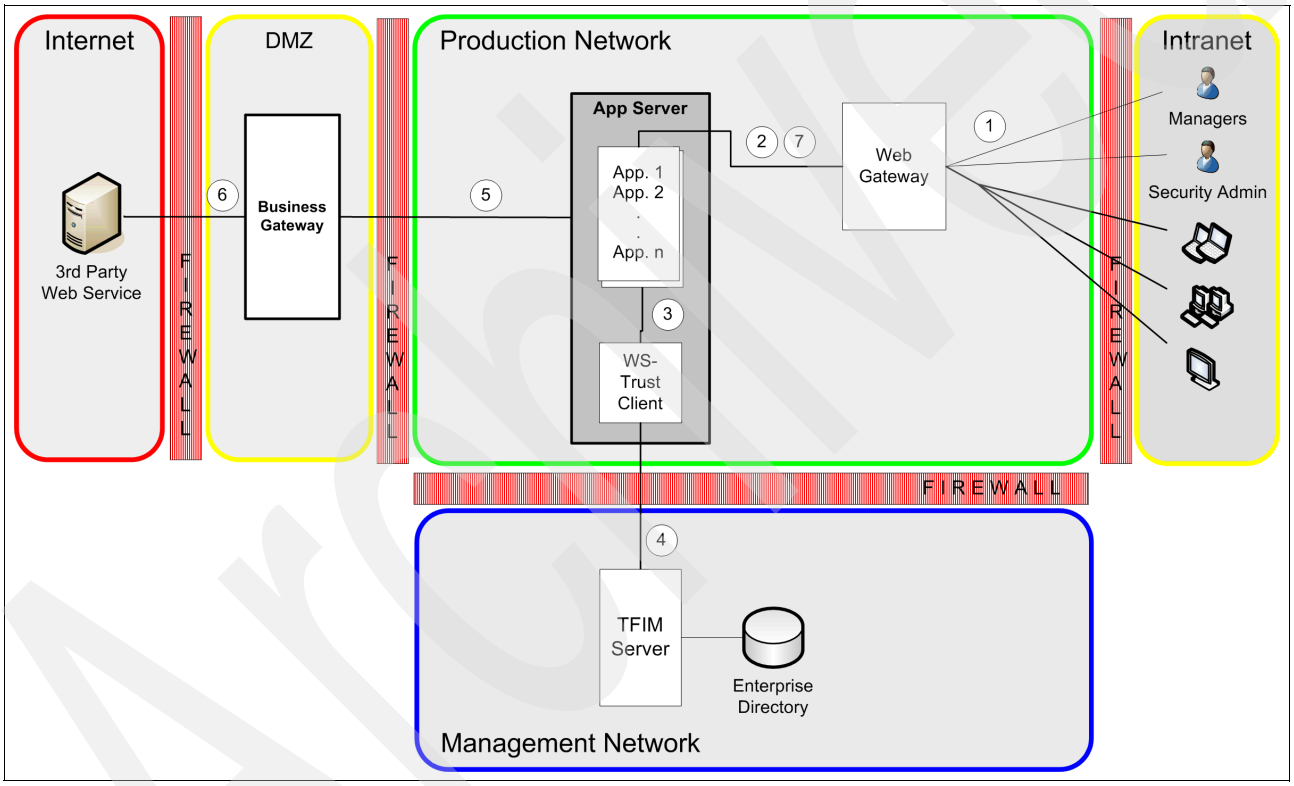

Figure 2-6 Phase 1 implementation architecture

With Tivoli Federated Identity Manager, the healthcare provider can address the following issues:

- Reduce identity and security management costs through linkage and reuse between organizations. The healthcare provider and its business partners no longer must separately manage common user attributes, which can help reduce identity life-cycle management costs and compliance concerns.
- Simplify the user experience because authorized employees can easily retrieve data that is provided by partner organizations, based on a single authentication event.

- Extend the breadth of services available to employees and, with that, increase the information available in the proper context to provide additional value from the enterprise portal.
- Maintain strict controls on sensitive data by ensuring the appropriate access control decisions are made based on individual user credential and entitlement information.

> **More information:** For more information about federated identity management concepts and types of configurations, see *Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions*, SG24-6394.

Data flow

As you read through the following data flow, refer to Figure 2-6 on page 39.

1. A healthcare employee accesses the enterprise portal through a *web gateway* (this can be a security server to provide an additional layer of security, for example, Tivoli Access Manager for e-business WebSEAL).
2. After the user has been authenticated and his credentials are sufficient, the web gateway grants the request and redirects the user to the enterprise portal page hosted on the application server.
3. At the enterprise portal, the employee selects an application portlet that requires making a web service request for information from a third party (for example, lab test results, patient allergy data, or pre-existing conditions). The enterprise portal uses a WS-Trust Client to exchange the user credential on the enterprise portal for a credential in a format accepted by the web service provider.
4. The WS-Trust Client contacts the Secure Token Service (STS) hosted on the Tivoli Federated Identity Manager to exchange the user credential. A common scenario is to exchange a Lightweight Third Party Authentication (LTPA) or Kerberos token for a *SAML assertion*. SAML assertions provide the benefits of being standards-based to allow for heterogeneous platform integration and also provide for credential enrichment by allowing additional attributes to be passed within the credential.
5. A secured web services request containing the SAML assertion is sent from the enterprise portal to the third-party Web Service Provider. The request passes through a web service gateway (Business Gateway) in the DMZ to allow for appropriate message validation, routing, and transformation, and provides perimeter control at the boundary of the organization's security zone.
6. The web service provider receives the request and validates the credential token. If the credential validation and access control checks are successfully completed, the web service provider returns the appropriate response to the client request from the enterprise portal.
7. The enterprise portal displays the information to the user.

Implementation steps

The implementation steps for enabling access to third party business services are as follows:

1. Establish the trust relationship between the organizations creating the framework for extending the value-added services. The trust relationship is based on business, legal, and technical principles.
2. Document the business, legal, and technical requirements establishing which data will be exchanged and how it will be passed with the third party service provider. These requirements include the data to be accessed, security controls on the data and communication protocols, credential types used, and how compliance will be monitored and reported.

3. Install the Tivoli Federated Identity Manager components.
4. Configure the application server to use the WS-Trust Client to call the Tivoli Federated Identity Manager STS for identity credential exchange purposes.
5. Configure Tivoli Federated Identity Manager and the trust chain to exchange the user credential from the enterprise portal for a credential type that can be consumed by the web service provider.

2.3.2 Phase 2: Enabling federated identity-management-based access

Federated identity management with Tivoli Federated Identity Manager enables the healthcare organization users to access web application resources offered by solution partners without requiring an additional authentication on the Service Provider side. Tivoli Federated Identity Manager supports several federation protocols to foster the creation of trust relationships with partners. Using federated identity management, an *Identity Provider* performs the authentication step and *asserts* an identity with the user request that the *Service Provider* can *consume* and validate based on the trust relationship information previously shared between the partners. This approach facilitates the user management on the Service Provider organization because they do not need to maintain passwords for the user to support the authentication step. The authentication requirements are completed by the Identity Provider and trusted by Service Provider based on the business and technical agreement in place between the parties.

In this next phase, the user of the healthcare provider enterprise portal wants to connect to additional web application resources that are provided by insurance and claim processing partners. By establishing trust relationships with these organizations, users who authenticate to the enterprise portal can seamlessly access the web applications extended by the insurance and claim processing partners. The enterprise portal, serving as the Identity Provider, uses the SAML federated protocol and assertion type to provide, or assert, the identity of the requesting user. From the perspective of the users, their authentication to the enterprise portal has extended the breadth of resources available to them without requiring additional authentication steps. The insurance and claim processing partners also have the additional value of securely allowing access to web application resources without the need to manage user authentication credentials like passwords. This deployment example is depicted in Figure 2-7 on page 42.

Technical requirements: The business partner requires a technology that supports federation protocols such as those used by Tivoli Federated Identity Manager, Tivoli Federated Identity Manager Business Gateway, or other vendor solutions. The key to deriving value from the solution is found by using a standards-based approach, allowing the partner (or partners) not to be tied to a specific vendor.

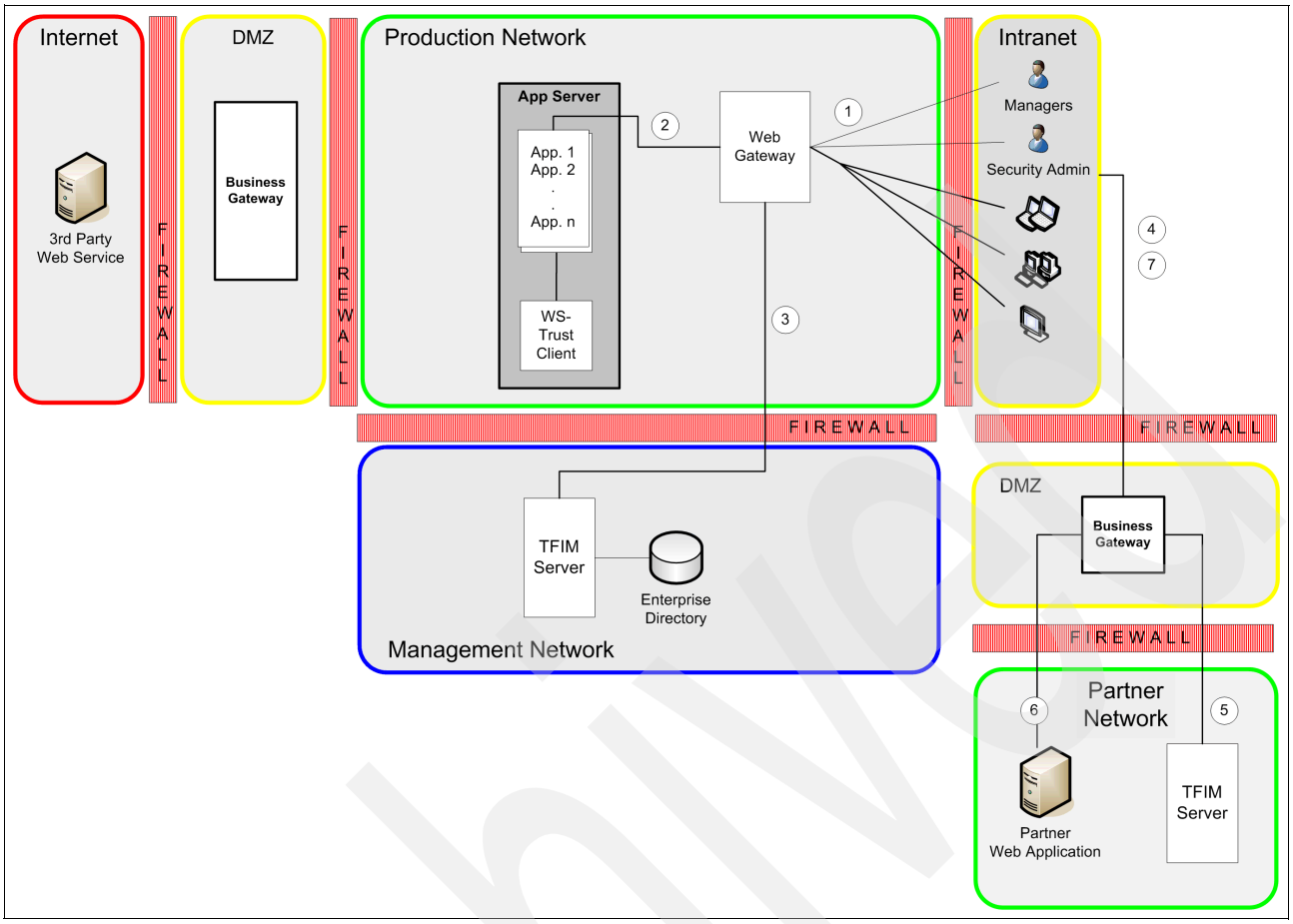

Figure 2-7 Phase 2 implementation architecture

As in Phase 1, with Tivoli Federated Identity Manager, the healthcare provider can address the following issues:

- Reduce identity and security management costs through linkage and reuse between companies. The provider and its business partners no longer need to separately manage common users, thereby helping to reduce identity life-cycle management costs.
- Simplify user experience because authorized employees can easily retrieve data provided by partner organizations based on a single authentication event.
- Extend the breadth of services available to employees increasing the information available in the proper context, hence allowing additional value to be derived from the enterprise portal.
- Maintain strict controls on sensitive data by ensuring the appropriate access control decisions are made based on individual user credential and entitlement information.

Data flow

As you read through the following data flow, refer to Figure 2-7.

1. A healthcare employee accesses the enterprise portal through a web gateway.
2. The user selects a link on the enterprise portal for an application that is provided by a business partner.
3. Acting as the Identity Provider point of contact, the web gateway contacts the Tivoli Federated Identity Manager server to generate the appropriate communication protocol

and token type for the business partner that is hosting the application: the Service Provider. This step includes redirecting the user browser to the partner application with the appropriate credential for the Service Provider to consume. In this case, the Identity Provider and Service Provider have previously agreed to use SAML as the protocol and assertion type for creating the federated identity management relationship. The appropriate configuration information and encryption keys have been exchanged between the parties in advance.

4. The user browser sends the request formatted by the Identity Provider to the Service Provider, which is hosting the web application that was originally requested on the enterprise portal.
5. The Service Provider receives the requests and uses its Tivoli Federated Identity Manager server to consume the request and validate the credential based on the information previously exchanged with the Identity Provider. If successfully completed, a local user context for the Service Provider is created for the user.
6. The user is then redirected to the business partner web application without the need to authenticate again. The trust relationship established between the business partners allows for seamless and secure access of the application to the user.
7. The business partner web application displays the page requested by the user.

Implementation steps

The implementation steps for enabling federated identity-management-based access are as follows:

1. Establish the trust relationship between the organizations based on legal, business, and technical principles.
2. Document the business, legal, and technical requirements to establish what data needs to be exchanged and how it is passed to the third party Service Provider. These requirements include the data to be accessed, security controls on the data and communication protocols, credential types used, and how compliance is monitored and reported.
3. Install the Tivoli Federated Identity Manager components.
4. Configure the web application to use the appropriate link to initiate the federated identity exchange.
5. Configure Tivoli Federated Identity Manager to support the federated identity exchange based on the technical requirements established with each business partner.

Switching roles: The healthcare provider can also use Tivoli Federated Identity Manager to participate as a Service Provider in a federated identity management relationship with a business partner. In this case, the healthcare provider uses Tivoli Federated Identity Manager to consume federation protocols and credentials from another partner serving as the Identity Provider who asserts the user identity.

2.3.3 Phase 3: Implementing centralized logging and reporting

To establish a centralized location for logs and creating reports, the healthcare provider chooses to implement centralized reporting and log management by using IBM Tivoli Security Information and Event Manager. In Figure 2-8 on page 44, the healthcare provider deploys a Tivoli Security Information and Event Manager (in the figure, TSIEM) server environment with an Agent in the Production Network. More technical details about Tivoli Security Information and Event Manager components are in 2.2, “Log and access management for audit readiness” on page 26.

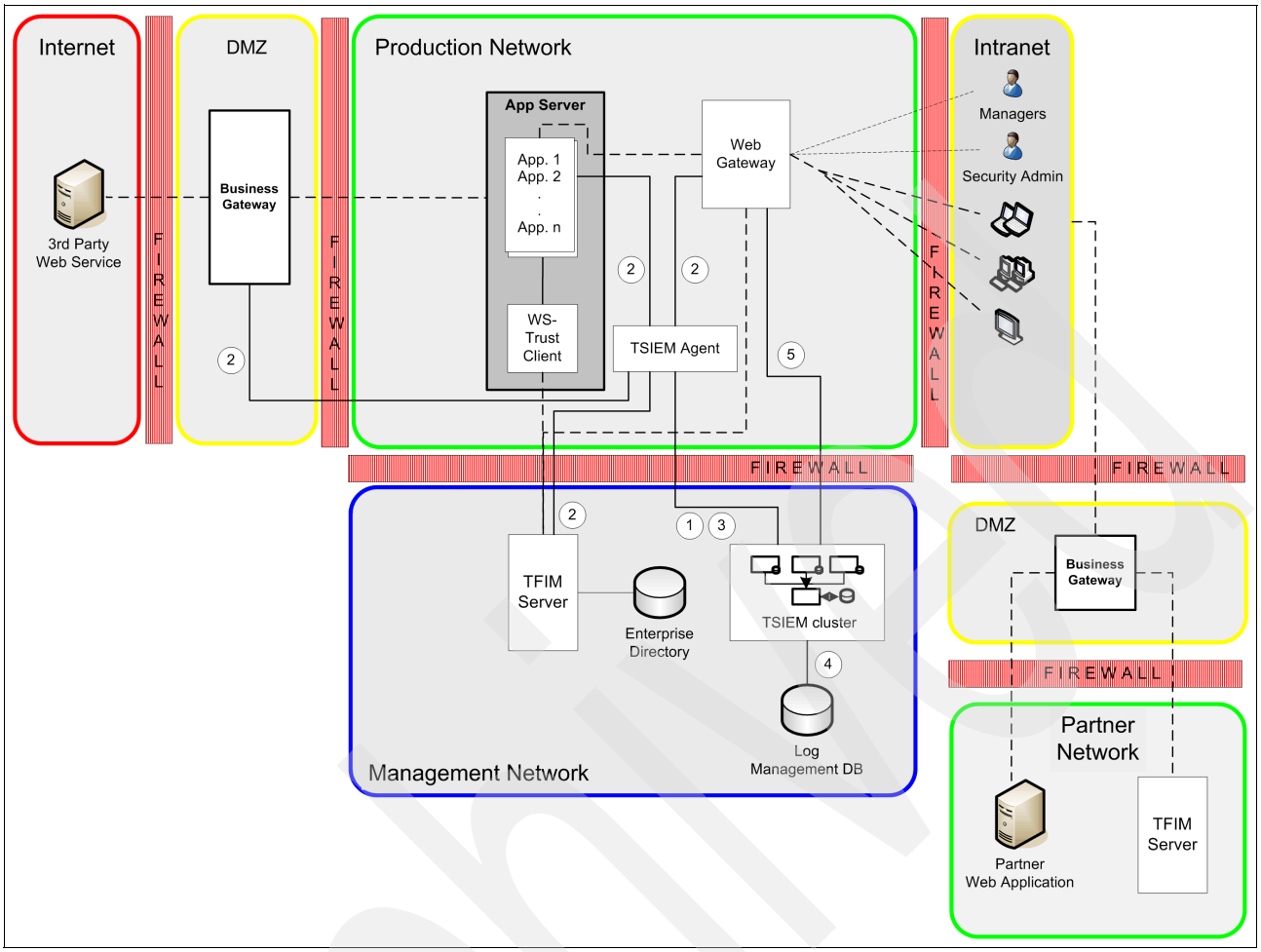

Figure 2-8 Phase 3 implementation architecture

With Tivoli Security Information and Event Manager, the healthcare provider can address the following issues:

- Enable a robust log collection and management system throughout the distributed IT environment. This includes monitoring existing applications, operating systems, and databases.
- Monitor and report user access to patient records (and other sensitive information) to ensure that confidentiality, integrity, and the availability of data and systems is properly maintained. The sensitive records that needed monitoring for regulatory compliance include patient medical data in addition to financial data stored on the provider's systems.
- Monitor and report on privileged users and their activities on key systems and data in the organization.

Data flow

As you read through the following data flow, refer to Figure 2-8.

1. The collection schedule is triggered automatically based on configured settings. Alternatively, a manual collection command can be given to the Tivoli Security Information and Event Manager server through the Management Console. The Tivoli Security Information and Event Manager server issues an audit trail collect command to the Agent. This command activates the Agent on the audited machines.

2. The appropriate script on the Agent reads the security log and collects only those new records since the last collection.
3. The Agent formats the collected records into a chunk format and compresses the chunks. A chunk can contain many log types from an audited machine. The Agent reads the chunk log data and securely sends the chunk data in encrypted form to the Agent on the Tivoli Security Information and Event Manager server.
4. The Agent on the server receives the chunk. The server application stores the chunk in the Depot and archives the chunks by registering them in the log manager application and configuration database. After successfully sending the chunks to the Tivoli Security Information and Event Manager server, the Agent deletes its local copy of the chunk. Additionally, on certain platforms, the Agent is set up to delete the original audit trail, when appropriate.
5. Managers and security administrators can access the Compliance Dashboard reporting application web interface to generate specific compliance reports and policy violation reports.

Implementation steps

The steps for implementing centralized logging and reporting are as follows:

1. Install the Tivoli Security Information and Event Manager server, and necessary Agents per platform type.
2. Activate auditing on the event source platforms sufficient to meet reporting needs.
3. Schedule and configure log collections from each log source.
4. Schedule and configure the loads of the log data into each W7 reporting database based on individual needs.
5. Review logs, such as the basic log reports, log continuity reports, log history, events by type, and so on.
6. Build the policy including attention rules (black list) and acceptable use-policy (white list).
7. Configure alerts.
8. Create and configure reports.

Repeat step 2 - 8 for all reports for each event source.

2.4 Conclusion

This chapter presented three distinct customer scenarios, each focusing on separate business or technical requirements. By exploring issues faced in various industries, the scenarios demonstrated how the IBM Tivoli Identity and Access Assurance offering can address one or all of the following challenges:

- Centralized user ID management
- Single sign-on identity management
- Federated identity management
- User access management
- Log and reporting management

IBM Tivoli Identity and Access Assurance offers a single-vendor solution to enterprise user identity management and reporting.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks

For information about ordering these publications, see “How to get Redbooks” on page 48. Note that some of the documents referenced here might be available in softcopy only.

- *Deployment Guide Series: IBM Tivoli Access Manager for e-business V6.0*, SG24-7207
- *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350
- *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014
- *Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions*, SG24-6394
- *Identity Management Design Guide with IBM Tivoli Identity Manager*, SG24-6996
- *IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager*, SG24-7530
- *Propagating Identity in SOA with Tivoli Federated Identity Manager*, REDP-4354

Online resources

These web sites are also relevant as further information sources:

- Product documentation for all IBM Tivoli products:

  http://publib.boulder.ibm.com/tividd/td/tdprodlist.html
- Product overview for the IBM Tivoli Identity and Access Assurance offering:

  http://www.ibm.com/software/tivoli/products/identity-access-assurance/

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, and order hardcopy Redbooks publications, at this web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Addressing Identity, Access, and Compliance Requirements

Using IBM Tivoli Identity and Access Assurance

Redpaper™

Introduces security solution and security management components

Describes tangible business benefits and investment returns

Provides customer deployment scenarios

Today, security is a concern for everyone, from members of the board to the data center. Each day another data breach occurs. These incidents can affect an organization's brand, investment return, and customer base. Time spent managing security incidents and managing risks can take time away from focusing on strategic business objectives. Organizations need to address security challenges by administering, securing, and monitoring identities, roles, and entitlements with efficient life-cycle management, access controls, and compliance auditing.

Those tasks include automated and policy-based user management to effectively manage user accounts and centralized authorization for web and other applications, and also enterprise, web, and federated single sign-on, inside, outside, and between organizations. Increasingly important requirements are the integration with stronger forms of authentication (smart cards, tokens, one-time passwords, and so forth) and centralizing policy-based access control of business-critical applications, files, and operating platforms.

This IBM Redpaper publication describes how the IBM Tivoli Identity and Access Assurance offering can help you address compliance initiatives, operational costs (automating manual administrative tasks that can reduce help desk cost), operational security posture (administering and enforcing user access to resources), and operational efficiencies (enhancing user productivity).

REDP-4548-00

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks