### **Knowledge Transfer (KT) Document : SRE**

#### Document Information

* Document Title: Jenkins, YCrash, Ansible, Peoplesoft Architecture, Payroll Engine, Okta, Service now, Monitoring Tools - Overview
* Version:1.1
* Date: 22nd Apr 2024 - 26thApr 2024
* Prepared By: SRE-Coforge
* Reviewed By: Satya Akella (Coforge)

Table of Contents

[**Knowledge Transfer (KT) Document : SRE** 1](#_Toc165225913)

[1.0 Introduction 2](#_Toc165225914)

[1.1 Purpose of Document 2](#_Toc165225915)

[1.2 Scope of KT 2](#_Toc165225916)

[1.3 Intended Audience 2](#_Toc165225917)

[1.4 Acronyms and Abbreviations 2](#_Toc165225918)

[**2.** Jenkins: 3](#_Toc165225919)

[3. YCrash 3](#_Toc165225920)

[4. Ansible 4](#_Toc165225921)

[5. Standard Operating Procedures (SOPs): 4](#_Toc165225922)

[Key URL’s mentioned : 6](#_Toc165225923)

[6. **Purpose of PeopleSoft at TriNet:** 6](#_Toc165225924)

[6.1 **Overall PeopleSoft Architecture:** 6](#_Toc165225925)

[6.2 Components of People Soft: 7](#_Toc165225926)

[6.3 Application Servers : 8](#_Toc165225927)

[6.4 Integration Broker : 8](#_Toc165225928)

[6.5 Process Scheduler : 8](#_Toc165225929)

[6.6. Obsolete Components: 9](#_Toc165225930)

[6.7. Transition to BODT (Oracle Managed Back Office): 9](#_Toc165225931)

[6.8 Production Environment Status: 9](#_Toc165225932)

[6.9. Database Architecture and Data Model: 9](#_Toc165225933)

[6.10. Server Roster and Environments: 9](#_Toc165225934)

[6.11. Server Architecture: 10](#_Toc165225935)

[6.12 Technology Stack: 10](#_Toc165225936)

[6.13 Tools Release vs. Application Release: 10](#_Toc165225937)

[6.14 Monitoring and Troubleshooting: 10](#_Toc165225938)

[6.15 Criticality of PeopleSoft: 11](#_Toc165225939)

[6.16 Introduction to Payroll Engine: 11](#_Toc165225940)

[6.16.1 Underlying Technology: 11](#_Toc165225941)

[6.16.2 Components of Payroll Engine: 11](#_Toc165225942)

[6.16.3 Functionality: 11](#_Toc165225943)

[6.16.4 Monitoring Payroll Engine: 11](#_Toc165225944)

[6.16.5 Stop and Start Procedures: 12](#_Toc165225945)

[6.17 PeopleTools 12](#_Toc165225946)

[6.17.1. Application Designer : 12](#_Toc165225947)

[6.17.2 Configuration Manager: 13](#_Toc165225948)

[6.17.3 Data Mover: 13](#_Toc165225949)

[6.17.3.1 Overview: 13](#_Toc165225950)

[6.17.3.2 Functionality: 13](#_Toc165225951)

[6.17.3.3 Usage: 13](#_Toc165225952)

[6.17.3.3 Access: 13](#_Toc165225953)

[6.17.3.4 Data Manipulation: 13](#_Toc165225954)

[**7. Okta:** 13](#_Toc165225955)

[7.1 Overview: 13](#_Toc165225956)

[7.2 Security Practices: 14](#_Toc165225957)

[7.3 Login Flow Diagram: 14](#_Toc165225958)

[7.4 Branding: 15](#_Toc165225959)

[7.3 Groups: 16](#_Toc165225960)

[7.4 Features in OKTA 16](#_Toc165225961)

[7.5 Rate Limiting : 18](#_Toc165225962)

[7.6 Security features in OKTA: 18](#_Toc165225963)

[7.7 Identity Providers(IDPs) : 18](#_Toc165225964)

[8. **Service Now :** 19](#_Toc165225965)

[8.1 Problem Management: 19](#_Toc165225966)

[8.2 Incident Management : 20](#_Toc165225967)

[8.3 Change Mangement : 21](#_Toc165225968)

[**9. Introduction to monitoring tools:** 22](#_Toc165225969)

[**9.1 OCI Monitoring Flow/Architecture:** 23](#_Toc165225970)

[**9.3 Key URL’s mentioned :** 24](#_Toc165225971)

# **1.0 Introduction**

### 1.1 Purpose of Document

This document serves the purpose of Overview of Technical Tools like Green stack Application, Peoplesoft, Ansible, Jenkins, YCrash, Service Now

### 1.2 Scope of KT

The scope is to cover detailed understanding of Techinical stack and responsibilities of SRE.

### 1.3 Intended Audience

SRE – Coforge Team

SRE – Trinet Team

### 1.4 Acronyms and Abbreviations

|  |  |
| --- | --- |
| Acronym | Full Form |
| GC | Garbage Collection |
| SLA | Service Level Agreement |
| RPA | Robotic Process Automation |
| HCM | Human Capital Management |
| FSCM | Financial & Supply Chain Management |
| IB | Integration Broker |
| IAM | Identity Access Management |
| MFA | Multi Factor Authentication |
| IDP | Identity Provider |
| DEM | Digital Experience Monitoring |
| OLA | Oracle logging Analytics |
| SSO | Single Sign On |

### **2.** Jenkins:

* Initially, Jenkins was implemented to automate the ForgeRock refresh process, which involved nightly database backups and restoration. This automation streamlined a lengthy manual process.
* TriNet SRE uses Jenkins for stopping and starting production applications, as well as for automating horizontal patching activities by integrating it with the Unix team's workflows.
* We have Jenkins instances for development and production environments. The development instance handles non-production environments, while the production instance is dedicated solely to managing production.
* **Horizontal Patching Process**: Through Jenkins, the Unix team makes API calls to Jenkins server to execute horizontal jobs. These jobs facilitate the stop and start of applications in a horizontal fashion, ensuring continuous availability during patching without bringing down the entire production environment.
* **Tableau Backup and Restore**: Another instance where Jenkins is utilized is for the backup and restore processes of Tableau.
* **RPA Team Integration**: The RPA team leverages Jenkins instances to manage their Automation Anywhere servers for backup and restoration.
* **Environment Management**: Your organization maintains separate Jenkins instances for development and production environments. The development instance handles non-production environments, while the production instance is dedicated solely to managing production.

### 3. YCrash

* YCrash is basically a comprehensive performance monitoring and diagnostics tool designed specifically for java applications.
* It is a tool to analyse the heap and thread dumps, GC logs in the application.
* Without YCrash tool we have to manually take the thread dumps and heap dumps and analyse those huge dumps which is tedious process.
* It offers insights into performance bottlenecks , memory leaks and other issues that can affect the reliability and efficiency of java based software systems.
* YCrash is automated with the AppDynamics by ServiceNow team so that AppDynamics will automatically trigger YCrash to take the heap and thread dumps.

### 4. Ansible

* Ansible was extensively used for various applications and technologies like WebLogic, Java, Jenkins, etc.
* Recent use cases include Tomcat and Java Version updates
  1. **Directory Structure:**
  + Playbooks are stored under the **Ansible** directory, with roles defined in the **roles** directory and variables in the **group\_vars** directory.
  + Inventory is defined in the **host files** directory.
  1. **Execution and Host Groups:**
  + Playbooks are executed against specific host groups defined in the inventory files.
  + Host groups are defined based on application components or layers, allowing for targeted execution.
  1. **Playbook Structure and Tasks:**
  + Playbooks define roles and variables, with tasks specifying actions to be performed.
  + Tasks include actions like creating staging directories, downloading and installing software, and configuring environment variables.
  1. **Handling Failures:**
  + Playbook executions may encounter failures, such as SSH connection issues or task failures.
  + Failed tasks or hosts can be re-run, and idempotent nature ensures consistent results upon re-execution.

# **5. Standard Operating Procedures (SOPs):**

* + The SRE team follows specific SOPs, including a single point of contact (on-call rotation), incident management, and response procedures.
  + SOPs also cover responsibilities such as daily health checks, password changes, environment switch-over events, and ransomware exercises.

**5.1 On-Call Rotation:**

* + The on-call rotation involves both onshore and offshore shifts, with specific hours.
  + Onshore – 9 AM – 9 PM CST
  + Offshore – 9PM -9 AM CST
  + The on-call person is the primary point of contact for incidents and coordinates the response, including engaging experts from various teams if necessary.

**5.2 Incident Management:**

* + Incidents are assigned to the on-call person initially, who then delegates them as needed.
  + The on-call person ensures incidents are resolved within SLAs and updates ServiceNow accordingly.
  + Lessons learned from incidents are discussed in team meetings to improve processes.

**5.3 Ransomware Exercises:**

* + The team conducts ransomware exercises to simulate real-world scenarios and test response procedures.
  + The goal is to restore critical functionality within a specified timeframe, with lessons learned and improvements made after each exercise.

**5.4**  **Demo Environment Support:**

* + The team supports demo environments used by the sales team for product demonstrations.
  + Weekly checks ensure the demo environment is healthy and functioning properly.

**5.5** **Monitoring and Observability:**

* + The on-call person monitors various tools for alerts and escalates issues as necessary.
  + Any gaps in observability are identified and addressed with the monitoring team to ensure comprehensive coverage.

**5.6** **SLA Compliance:**

* + SLAs for incident resolution are tracked through ServiceNow, with managers monitoring performance.
  + Incidents are assigned, updated, and resolved promptly to meet SLAs and avoid exceeding them.

**5.7** **Communication and Collaboration:**

* + Communication channels like team chat are used for warm handoffs between on-call shifts.
  + Team meetings and scrum calls facilitate communication of lessons learned and continuous improvement.

Overall, the SRE team follows a structured approach to incident management, ensuring efficient response, compliance with SLAs, and continuous improvement through regular exercises and feedback loops.

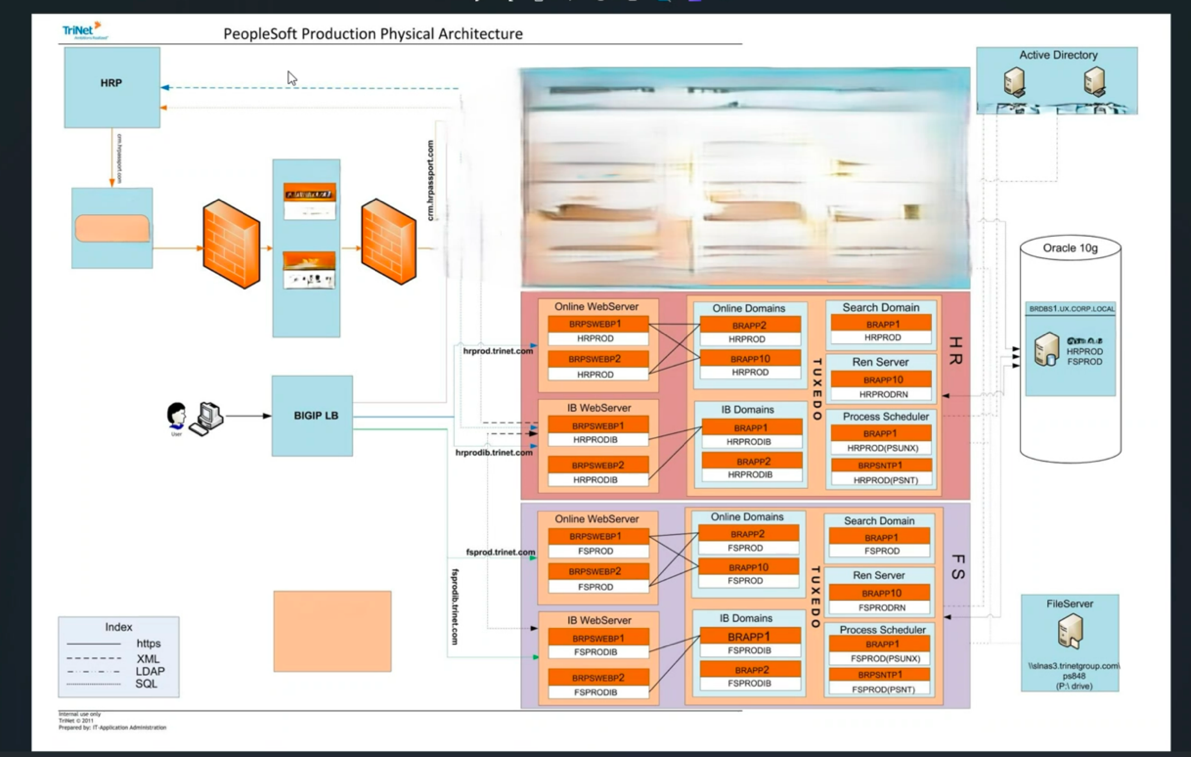
## Key URL’s mentioned :

On Call Prodedures for SRE : <https://confluence.trinet-devops.com/x/ZANsAw>

### 6. **Purpose of PeopleSoft at TriNet:**

* + PeopleSoft is crucial for TriNet's payroll generation, serving as a back-end tool for processing payroll and benefits.
  + It's considered a flagship application, historically categorized as an ERP tool for managing human resources-related processes.

### 6.1 **Overall PeopleSoft Architecture:**

* + PeopleSoft transition from on-premises data centers to Oracle Cloud Infrastructure (OCI) has occurred recently.
  + This application is in internal zone and not exposed to the world. End users can access with the Green stack Application.
  + People soft comprises of two main components such HR (HCM), and FS (FSCM) [FS is only in read only mode].
  + PeopleSoft architecture comprises web servers, application servers, process schedulers (or batch servers), and database servers.
  + Web servers handle user requests and load balancing via F5, communicating with application servers.
  + Application servers serve as the core of PeopleSoft, divided into domains such as Integration Broker (IB), process schedulers.
  + IB are used for messaging and data exchange.
  + Process schedulers manage batch jobs and scheduling tasks, utilizing separate engines for Unix and Windows environments.
  + Tuxedo middleware facilitates communication between web servers, application servers, and databases, processing requests and data retrieval.
  + 

### 6.2 **Components of People Soft:**

#### 6.2.1 Active Directory Integration:

* + Active Directory is utilized for user credential authentication.
  + PeopleSoft code interacts with Active Directory for user validation.
  + Once authenticated, PeopleSoft's own security mechanisms govern user access based on roles and permissions.
  + Microsoft Azure is utilized for authentication purposes.

#### 6.2.2 File Server:

* + Houses external files such as COBOL and SQL code.
  + COBOL files are extensively used for payroll and benefits processing.
  + Users access log files, code files, and other resources stored on the file server for troubleshooting and analysis.

#### 6.2.3 Web Servers :

* + Web servers handle user requests and load balancing via F5, communicating with application servers.
  + These servers are built on WebLogic .

### 6.3 Application Servers :

* + Application servers serve as the core of PeopleSoft, divided into domains such as Integration Broker (IB), process schedulers.
  + They run with the help of TUXEDO middle tier tool which sends all requests between Webserver and DB.

### 6.4 Integration Broker :

* + Integration brokers in PeopleSoft are components designed to facilitate the exchange of data between PeopleSoft applications and other systems, both within and outside an organization.

### 6.5 Process Scheduler :

Process Scheduler is a component that manages and schedules batch processes, reports, and other tasks across the PeopleSoft application. It ensures that processes are executed at the appropriate times and with the necessary resources.

Here's an overview of Process Scheduler in PeopleSoft:

#### 6.5.1 Batch Processing:

* Process Scheduler handles batch processing tasks such as running overnight processes, generating reports, and performing data extracts or integrations.
* These tasks are typically time-consuming or resource-intensive and are better suited for batch processing rather than interactive processing.

#### 6.5.2 Scheduling:

* Process Scheduler allows administrators to define schedules for running batch processes. Schedules can be based on various factors such as time of day, day of the week, or specific dates.
* Recurring schedules can also be set up for processes that need to run on a regular basis.

### **6.6. Obsolete Components:**

* + Certain components like the CRM product have been deprecated, with focus primarily on the HCM module.
  + Ren Server also completely obsolete.

### **6.7. Transition to BODT (Oracle Managed Back Office):**

* + Finance activities have transitioned to BODT, Oracle's managed back office solution.
  + Finance operations are now primarily handled through BODT, with existing finance domains in a read-only mode for verification and comparison purposes.

### 6.8 Production Environment Status:

* + Finance domains have been removed from lower environments but still exist in production for specific activities.
  + Finance activities are gradually transitioning to ODT, with plans to phase out the finance domains entirely.

### **6.9. Database Architecture and Data Model:**

* + PeopleSoft and Passport may share some common data, such as employee information, but each serves distinct purposes.
  + A data flow diagram or data model showcasing the data stored in each system could provide clarity on the differences and overlaps.
  + While PeopleSoft primarily manages HR-related data, Passport focuses on user configurations, benefits, and payroll processing.

#### 6.9.1 Data Refresh and Maintenance:

* + Historically, data refreshes were conducted in PeopleSoft, but TriNet has transitioned to synthetic data and code catch-up approaches.
  + DBA and Unix teams collaborate closely to maintain database health and application uptime.
  + SRE (Site Reliability Engineering) teams oversee the overall health of the application and coordinate with DBAs and Unix teams to address any issues.

### **6.10. Server Roster and Environments:**

* + TriNet's PeopleSoft environment includes various production, staging, testing, and demo environments.
  + Production environments include HR prod, FS prod, HR prod history, HR light, and a sales demo environment.
  + Staging environments include stage 1, stage 2, and critical environments like perf one for performance testing.
  + Other environments like dev, LTE, demo one, QE1, QE2, QE3, Vanilla, AWS-based environments, tax environment, and vanilla environment are also used for different purposes.

### **6.11. Server Architecture:**

* + Each environment typically consists of web servers, application servers (running WebLogic or Tuxedo), process schedulers, and sometimes PST servers (Windows-based equivalents).
  + Servers are grouped into different tiers based on their functions, such as web servers, app servers, and process schedulers.
  + LTE environment serves as a clone of production, refreshed nightly, and used for troubleshooting real-time issues.
  + Demo environments like demo one are used by the sales team to showcase the platform to potential clients.
  + QE environments are utilized by engineering and QA teams for development and testing purposes.

### **6.12 Technology Stack:**

* + Web servers typically run on WebLogic, while app servers run on Tuxedo.
  + The SRE team is responsible for managing and configuring these servers, while external teams like Linux or network teams are called upon for specific issues beyond the SRE's scope.

### **6.13 Tools Release vs. Application Release:**

* + PeopleSoft environments have both tools release and application release.
  + The tools release stores technical metadata, while the application release stores business data like HR, payroll, and benefits information.
  + Updates and patches can be applied separately to tools release and application release.

### **6.14 Monitoring and Troubleshooting:**

* + Monitoring tools like AppDynamics are used for database monitoring, while troubleshooting often involves analyzing log files.
  + Cron jobs are crucial for monitoring and alerting, providing signals for any issues that need attention.
  + Server environments are predominantly hosted on Red Hat Linux.

### **6.15 Criticality of PeopleSoft:**

* + PeopleSoft is considered a core critical business process application, similar to other client-facing platforms.
  + SLAs and criticality of PeopleSoft align with core business processes, emphasizing the importance of maintaining its stability and uptime.

Overall, the server roster, environments, and PeopleSoft application form a crucial part of TriNet's infrastructure, supporting various business processes and internal operations.

### **6.16 Introduction to Payroll Engine:**

It's a custom-built tool developed by TriNet to automate and enhance the efficiency of the payroll process for all Work Site Employees (WSEs).

### **6.16.1 Underlying Technology:**

PeopleSoft delivers payroll processes mainly in COBOL, a compiled language known for its fast batch processing capabilities.

### **6.16.2 Components of Payroll Engine:**

It consists of three C programs - monitor, scheduler, and pay engine - along with two shell scripts for starting and killing processes.

### 6.16.3 Functionality:

* 1. **Pay Eng Monitor**: Checks the status of payroll engine across nodes and ensures they are running as expected.
  2. **Pay Eng Scheduler**: Distributes workload from the queue table to the appropriate engine, acting as a load balancer.
  3. **Pay Engine**: Executes specific tasks based on payroll parameters like pay group, pay date, and payroll number.

### **6.16.4 Monitoring Payroll Engine:**

* Users can monitor the engine's status through the Engine Monitor page, which displays active processes, available nodes, and workload distribution.
* Payroll Engine settings in PeopleSoft also provide insights into engine status and health.

### 6.16.5 **Stop and Start Procedures:**

* To shut down the engine, users first turn off the ignition, then execute the kill command, and finally start the engine back up.
* The sequence ensures a smooth transition and prevents data loss or corruption.

Overall, the payroll engine plays a critical role in streamlining payroll processing for a large number of employees, with robust monitoring, maintenance, and support mechanisms in place to ensure smooth operations.

### **6.17 PeopleTools**

* People tools provides the underlying technology for PeopleSoft applications.

All PeopleSoft applications, such as Human Capital Management and Customer Relationship Management are built, deployed, and maintained using PeopleTools. 

The PeopleTools suite includes tools like Application Designer, Configuration Manager, and Data Mover, among others.

### **6.17.1. Application Designer :**

Application Designer is a tool primarily used by developers for PeopleSoft application development and maintenance.

6.17.1.1 Components:

It includes various components like records, SQL tables/views, PeopleCode, and App Engine programs.

6.17.1.2 Usage:

Developers use it extensively for coding, development, and making changes to the application structure.

6.17.1.3 Access:

Access to Application Designer is set up through Configuration Manager, where database connections are configured

6.17.1.4 Development Activities:

Developers use it for creating and modifying table structures, writing PeopleCode, and developing App Engine programs.

6.17.1.5 Troubleshooting:

SREs also use Application Designer to troubleshoot issues related to table structure mismatches or data loading problems.

### **6.17.2 Configuration Manager:**

* Config Manager is used to configure the local environment for accessing Application Designer. It requires setting parameters like database name, user ID, and connect password.
* Once all necessary configurations are set up in Config Manager, the setup process is complete, and developers can start using Application Designer for development and maintenance tasks.

### 6.17.3 Data Mover**:**

### Overview:

* + Data Mover is a tool used for moving data in and out of the PeopleSoft application.

### Functionality:

* + It performs tasks such as data insertion, updates, and deletion, as well as moving data between PeopleSoft instances.

### 6.17.3.3 Usage:

* + SREs may use Data Mover for fixing data issues, applying patches, or migrating data between environments.

### Access:

* + Similar to Application Designer, access to Data Mover is configured through Configuration Manager.

### Data Manipulation:

* + It provides a mechanism for manipulating data directly in the database, making it a useful tool for data-related tasks.

### **7. Okta:**

### 7.1 Overview:

Okta is an Identity and Access Management (IAM) solution offered as a Software-as-a-Service (SaaS) offering, used for authentication, authorization, and user lifecycle management.

**Benefits of IAM Solutions**: IAM solutions like Okta offer numerous benefits, including regulatory compliance, robust security features, logging and analytics, and easy plug-and-play integration.

**Key Features of Okta**: Features such as Multi-Factor Authentication (MFA), sign-on policies, password rules, DDoS attack prevention, scalability, logging and reporting, Single Sign-On (SSO) connectors, social authentication, and APIs/SDKs are provided by Okta.

**Security**: Okta provides various security features and algorithms to detect and prevent malicious activities, ensuring a secure authentication process.

**Scalability**: Being a SaaS solution, Okta offers scalability without the need for manual infrastructure upgrades, ensuring seamless service delivery even with a growing user base.

**User Lifecycle Management**: Okta enables efficient management of the user lifecycle, from onboarding to offboarding, ensuring smooth user access management.

**Usage at TriNet**: At TriNet, Okta is utilized for customer identity and access management, providing a seamless login experience for end users accessing hrpassport.com.

### **7.2 Security Practices:**

**Importance of Security**: Maintaining security is crucial due to the sensitive nature of the data handled, such as customer information.

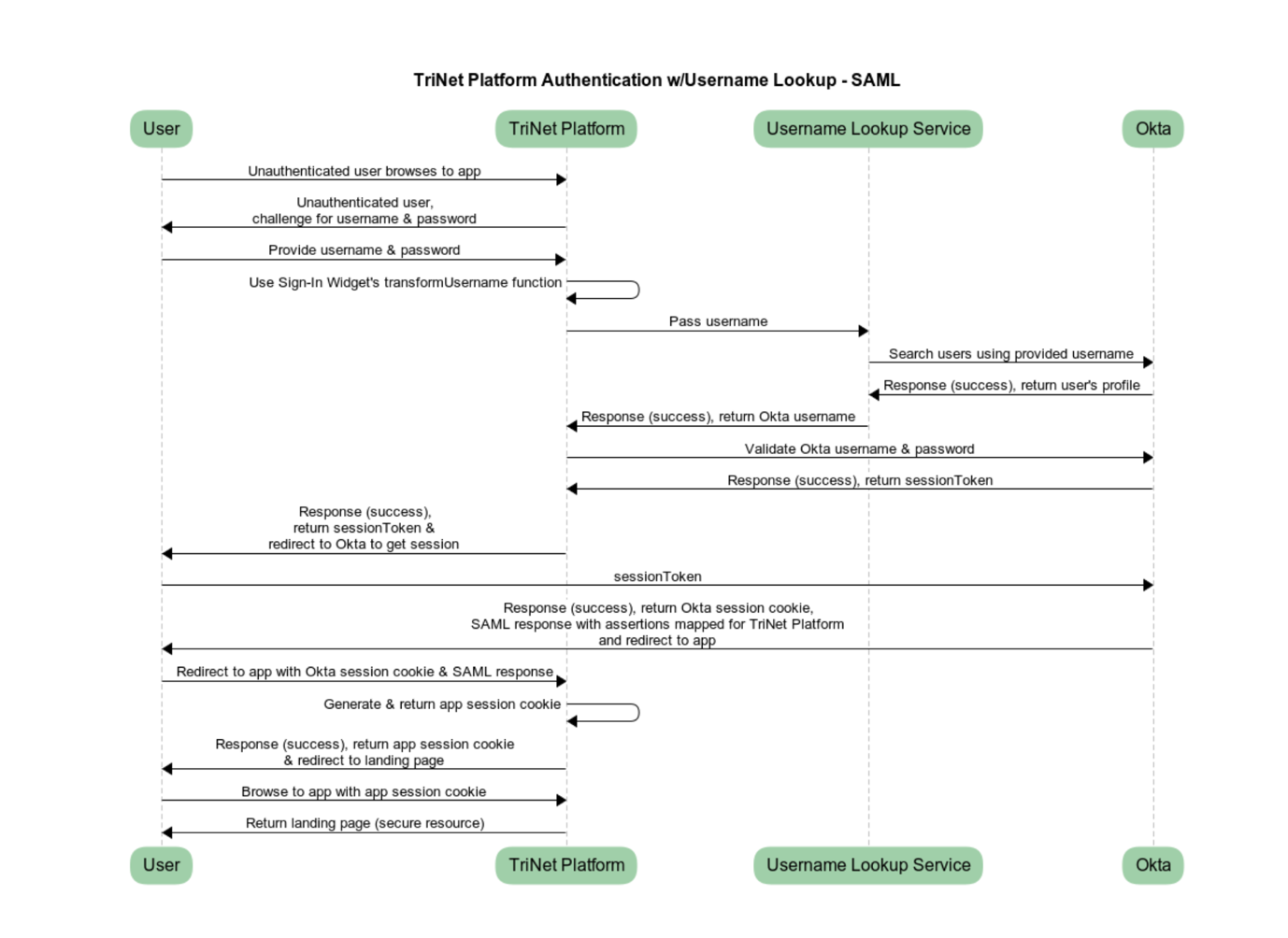
**Avoid Sharing Credentials**: It's essential **not to share credentials with anyone** and to be cautious about who has access to sensitive information.

**Physical Security Measures**: Avoid writing down passwords or leaving systems unlocked, as it can lead to unauthorized access.

**Training on Privacy and Security**: Emphasize the importance of privacy and security through core training sessions to maintain trust with clients and uphold the company's reputation.

### **7.3 Login Flow Diagram:**

* The login flow diagram illustrates the sequence of steps involved in the login process, including user authentication, authorization, and access to the application.



**End User Interaction**: The user initiates the login process by accessing hrpassport.com.

**Arcose Verification**: A call is made to Arcose for additional security verification, returning a token based on the risk profile.

**Authentication**: The user enters their credentials, which are routed through internal networks before reaching Octa for authentication.

**Multi-Factor Authentication (MFA)**: If necessary, OKTA prompts the user for MFA verification via email or SMS.

**Authorization**: Upon successful authentication, OKTA verifies the user's access privileges and grants a session token.

**Access to Resources**: The user gains access to the platform based on their authentication and authorization status.

Overall, prioritizing security measures and understanding the login flow process are crucial for maintaining the integrity and confidentiality of user data in the system.

### **7.4 Branding:**

**Custom Branding**: OKTA allows customization of the end-user experience through branding options.

**Branding Elements**: Logos, color patterns, and other visual elements can be customized for the login page.

**Page Customization**: Pages like sign-in pages can be customized to enhance the user experience.

**Email Templates**: Default email templates provided by OKTA can be customized to fit specific communication needs.

**Custom Domains**: Custom domains can be set up for branding purposes, providing a personalized URL for users.

**Certificate Management**: SSL certificates are managed and renewed periodically to ensure secure connections.

### **7.3 Groups:**

**Logical Segmentation**: Groups are used to logically segregate users based on their roles or entitlements.

**Application Assignment**: Applications can be assigned to groups, allowing easy management of user access to multiple applications.

**Purpose of Groups**: Groups streamline application assignment processes and facilitate effective access management.

Overall, OKTA provides robust branding options, group management features, and security policy configurations to ensure a personalized yet secure user experience. These elements play a crucial role in enhancing usability, access management, and overall security posture within the Octa platform.

### **7.4 Features in OKTA**

**7.4.1 MSA Flow for Admin Users :**

Admin users, regardless of their role, are required to go through a multi-step authentication (MSA) flow. This involves receiving a code on their primary email for verification.

**7.4.2 Network Zones:**

Network zones are used to control access to Okta based on IP addresses or IP ranges. Trusted IP addresses, such as those from Cloudflare, are allowed, while others may be blocked or restricted.

**7.4.3 Behaviour Detection :**

Okta offers behaviour detection features to identify risky user behaviour based on various parameters. However, this feature is not extensively used due to reliance on other security measures like Cloudflare.

**7.4.4 System Logs and Monitoring:**

The system log in Okta captures all events, including user authentication attempts, session changes, and administrative actions. Monitoring these logs is crucial for security and troubleshooting purposes.

**7.4.5 User Lifecycle Management :**

Admins handle user provisioning and deprovisioning, ensuring that users have appropriate roles and access levels based on their responsibilities. This process may involve manual actions or integration with other tools like ServiceNow.

**7.4.6 API Tokens :**

* API tokens are used by applications to interact with Okta's APIs for user management tasks. These tokens are securely managed and have specific permissions based on the role of the account that creates them.
* **Segregation of Duties:** Different types of API tokens are created by different accounts (e.g., app admin, deployment), each with specific privileges based on the role of the account.

**7.4.7 Logging and Monitoring :**

* Understanding and utilizing Okta's logging features, including system logs and event monitoring, are essential for maintaining security and compliance.
* All actions performed against Okta are logged extensively. Every single action is logged, making the logging process quite aggressive.

**7.4.8 User Deletion Policy :**

* There's a distinction between policies for administrators and end-users. For administrators, there's a check if the admin user hasn't been logged in for a certain period (e.g., 60 or 90 days).
* For end-users, deletion policies aren't applied uniformly due to factors like financial statements retention requirements.

**7.4.9 Login Events:**

* The log displays events such as successful or unsuccessful login attempts, evaluation of sign-on policies, and verification of user identity. Tokens like ID token, access token, and refresh token are issued upon successful login.

**7.4.10 Token Usage:**

* ID token contains identity information, access token specifies the user's access permissions, and refresh token is used to maintain session continuity without reauthentication after a period of inactivity.

**7.4.11 Retention Period for Logs:**

* Okta retains logs for 90 days, and currently, there's no external streaming of logs for retention or analytics purposes.

### **7.5 Rate Limiting :**

Rate limiting is a crucial concept for APIs, including Okta's API. It involves setting a maximum number of requests per minute for specific endpoints to enhance security and manage pricing.

**7.5.1 Security Enhancement :**

* Rate limiting helps in detecting and mitigating DDoS attacks by limiting the number of requests a bad actor can make. It helps in identifying unusual spikes in traffic and prevents malicious activities.

**7.5.2 Pricing Consideration :**

* Rate limits also play a role in pricing, as organizations with larger user bases may require higher rate limits, leading to potential adjustments in pricing by Okta.

**7.5.3 Dynamic Rate Limit Adjustments:**

* To prevent one client from consuming a disproportionate share of the rate limit, there may be conditions set to temporarily block users who exceed a certain threshold, ensuring fair access to the API.

**7.5.4 Handling Rate Limit Events:**

* Whenever the rate limit is reached or exceeded, Okta sends notifications, allowing administrators to investigate whether it's due to a security threat or genuine user activity.

### 7.6 **Security features in OKTA:**

**7.6.1 Threat Insights:**

* Okta's Threat Insights feature helps in identifying and blocking malicious traffic. Administrators can choose to log such attempts or enforce immediate blocking based on certain conditions.

**7.6.2 IP Change Detection and Security :**

* Okta provides features like IP change detection to enhance security. Admins can customize security settings to mitigate risks associated with malicious activities.

**7.6.3 Monitoring and Reporting:**

* Admins can monitor rate limit usage, security events, and other metrics through dashboards and reports provided by Okta. They can also receive notifications for any service disruptions or downtime.

### **7.7 Identity Providers(IDPs) :**

* IDPs enable single sign-on (SSO) for users. Different IDPs can be configured for various purposes, such as internal users or social logins.
* Azure AD is used as an IDP for internal users, facilitating SSO with Active Directory.
* Routing rules determine how users are authenticated based on criteria such as domain, device, or location. Users are routed to different IDPs for authentication based on these rules.

Overall OKTA provides complete customization for authorisation and authentication of users with features such as Multi-Factor Authentication (MFA), sign-on policies, password rules, DDoS attack prevention, scalability, logging and reporting, Single Sign-On (SSO) connectors, social authentication.

### 8. **Service Now :**

Introduction:

ServiceNow is a cloud-based platform that provides solutions for IT service management (ITSM). ServiceNow is used for tracking various processes like incident management, change management, and problem management. It helps organizations automate their workflows, streamline processes, and improve service delivery across various departments. ServiceNow offers modules for managing incidents, problems, changes, assets, and more, all within a single platform.

### 8.1 Problem Management:

Problem ticket is created after a production event to conduct a detailed analysis and identify the root cause of the issue. It aims to prevent the problem from recurring.

**8.1.2 Root Cause Analysis:**

The goal of a problem ticket is to get to the bottom of the issue, identify the root cause, and conduct a thorough analysis to prevent its recurrence.

**8.1.3 Problem Tasks:**

Problem tickets may involve multiple teams, each assigned specific tasks to address the root cause and prevent future occurrences.

**8.1.4 Collaboration with Teams:**

Collaboration with monitoring and observability teams is crucial to address issues effectively. Monitoring can be set up to alert teams immediately if similar issues arise in the future.

**8.1.5 ServiceNow Tasks:**

ServiceNow tasks involve provisioning and deprovisioning user accesses, ensuring proper access management and security measures.

**8.1.6 Weekly Reports and Dashboards:**

Weekly reports and dashboards are provided to management, detailing incident counts, SLA agreements, and other metrics. These reports help track performance and identify areas for improvement.

**8.1.7 SLA Compliance:**

Timely resolution of incidents is essential to meet SLA agreements. Keeping incidents updated and closing them promptly is necessary to avoid SLA warnings and maintain accurate metrics.

**8.1.8 ServiceNow Filters:**

ServiceNow allows filtering of previous tasks for reference or analysis, enabling teams to track past incidents or changes for learning and improvement purposes.

* + 1. **Adherence to Process:**

Adherence to the process is crucial, especially in change management. Changes must be properly documented and approved to ensure stability and security in production environments.

### 8.2 Incident Management :

**ServiceNow Incident Management:**

Incidents are reported through ServiceNow, where users describe the problem they're facing. The incident is then assigned to the appropriate team for resolution.

**8.2.1 SLA and Prioritization:**

Incidents are classified based on their severity, such as P1 for critical issues, P2 for urgent issues, and so on. Each severity level has corresponding SLA response and resolution times.

**8.2.2 Ticket Routing:**

Incidents are assigned to on-call personnel who acknowledge and address them accordingly. Primary and secondary on-call individuals are responsible for handling tickets during their shifts.

**8.2.3 Incident Acknowledgment and Resolution:**

On-call personnel must acknowledge and resolve incidents within the defined SLA times. Detailed notes and attachments should be added to incidents for future reference.

**8.2.4 Priority Adjustment:**

If an incident is misclassified, it can be adjusted to the appropriate priority level. For example, a non-prod incident mistakenly classified as P1 should be downgraded to P3 or P4.

 Justification for Priority: Justification may be required when creating high-priority incidents to ensure proper classification and resource allocation.

**8.2.5 Ticket Closure:**

Once an incident is resolved, it should be promptly closed with detailed notes. Keeping resolved incidents open can trigger SLA warnings and affect team performance metrics.

### 8.3 Change Mangement :

**8.3.1 Change Requests:**

Changes should be initiated through change requests for any activity involving alterations, such as disabling settings or running SQL queries in production. Change requests ensure proper approval and documentation.

**8.3.2 Types of Changes:**

Different types of changes include normal changes, decommission changes, outage changes, network changes, and emergency changes. Each type has its own process and criteria.

**8.3.3 Risk Assessment:**

When creating a change request, it's crucial to assess the risk accurately. Low-risk changes may not require extensive approval processes, while high-risk changes need thorough review.

**8.3.4 Approval Process:**

Change requests undergo various approval stages, including initial approval, change control board (CCB) review, and implementation approval. The approval process ensures that changes are carefully evaluated before implementation.

**8.3.5 Scheduling and Implementation:**

Changes should be scheduled to minimize disruption and avoid conflicts with other activities, such as production patching. The best time for implementation is determined through collaboration and conflict resolution meetings.

**8.3.6 Communication:**

Effective communication with stakeholders is essential throughout the change management process. It ensures that everyone is aware of planned changes and their potential impact.

**8.3.7 Testing and Validation:**

Changes should be thoroughly tested in non-production environments before implementation in production. Testing helps identify issues early and ensures a smooth transition to production.

Remember, following the process diligently ensures stability, security, and efficiency in managing IT operations.

### **9. Introduction to monitoring tools:**

TriNet uses a wide variety of monitoring tools to ensure end to end observability of their infrastructure and applications. These include infrastructure monitoring solutions, log monitoring solutions, application monitoring solutions. Below are the tools used by TriNet in PEO, DCP and HRIS environments respectively.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **PEO** | |  | **DCP** | |  | **HRIS** | |
| **Capability** | **Tool** |  | **Capability** | **Tool** |  | **Capability** | **Tool** |
| Infra/Metrics Monitoring | Prometheus(Alert Manager and Blackbox Exporter) & Grafana |  | Infra/Metrics Monitoring | AWS CloudWatch, AWS Managed Prometheus, AWS Managed Grafana & Datadog (Payroll) |  | Infra/Metrics Monitoring | Datadog & AWS CloudWatch |
| Log Monitoring | Oracle Logging Analytics (OLA) |  | Log Monitoring | AWS CloudWatch, AWS OpenSearch, Datadog (Payroll) |  | Log Monitoring | Datadog & AWS CloudWatch |
| APM | AppDynamics |  | APM | AppDynamics for BPL, BSS |  | APM | NA |
| Session Replay | Log Rocket |  | Error Tracing | Sentry |  | Error Tracing | Sentry |
| DEM | ThousandEyes |  | DEM | Nothing setup yet |  | DEM | ThousandEyes (Pingdom is being retired) |
| Notifications | ServiceNow Notify |  | Notifications | ServiceNow Notify (ServiceNow integration pending) |  | Notification | PagerDuty (Being replaced by ServiceNow) |

* **Infrastructure monitoring:** It is widely taken care by Prometheus and Grafana along with tools like BlackBox exporter, Datadogs.
* **Application performance monitoring:** It is mostly taken care by AppDynamics along with Datadogs.
* **Session replay(PEO):** Done through Log Rocket(However it is not managed by SRE Observability).
* **Digital Experience Monitoring(DEM):** We leverage ThousandEyes to monitor Trinet’s DEM as it offers with a huge number of collectors worldwide to monitor DEM.
* **Log Monitoring:** Trinet mostly utilizes native tools like AWS Cloudwatch, AWS OpenSearch, Oracle logging analytics for Log monitoring.
* Error Tracing: Sentry is used to further help with error tracing and is not managed by SRE Observability.

### **9.1 OCI Monitoring Flow/Architecture:**

Monitoring is done and visualised through multiple instance of Prometheus(4 instances) and Grafana(2) across the environments. Further all these alerts are further sent to ServiceNow which then sends notifications to necessary stakeholders on behalf of these alerts/events.



### **9.3 Key URL’s mentioned :**

|  |  |
| --- | --- |
| **Monitoring Tool** | **Link to access the tool** |
| Grafana - Non-Prod (OCI hosted) | <https://pa1graph01.ux.corp.local:3000/>  Use AD Credentials to login  [Grafana and Oracle Logging Analytics Brown bag session-20230712\_120425-Meeting Recording.mp4](https://trinethr-my.sharepoint.com/:v:/r/personal/sampath_basireddy_trinet_com/Documents/Recordings/Grafana%20and%20Oracle%20Logging%20Analytics%20Brown%20bag%20session-20230712_120425-Meeting%20Recording.mp4?csf=1&web=1&e=lcQE8s) |
| Grafana - Prod (OCI Hosted) | <https://pa1graph02.ux.corp.local:3000/>  Use AD Credentials to login  [Grafana and Oracle Logging Analytics Brown bag session-20230712\_120425-Meeting Recording.mp4](https://trinethr-my.sharepoint.com/:v:/r/personal/sampath_basireddy_trinet_com/Documents/Recordings/Grafana%20and%20Oracle%20Logging%20Analytics%20Brown%20bag%20session-20230712_120425-Meeting%20Recording.mp4?csf=1&web=1&e=lcQE8s) |
| Prometheus - Non-Prod (OCI Hosted) | Dev VMs - Prometheus URL: <https://pa1prom01.ux.corp.local:9090/> Dev k8s - Prometheus URL: <https://pa1prom02.ux.corp.local:9090/> |
| Prometheus - Prod (OCI Hosted) | Prod VMs - Prometheus URL: <https://pa1prom03.ux.corp.local:9090/> Prod k8s - Prometheus URL: <https://pa1prom04.ux.corp.local:9090/> |
| OCI Blackbox Exporter and Alert Manager | Non-Prod Blackbox Exporter URL: <https://pa1bbexp01.ux.corp.local:9115/> Non-Prod Alert Manager URL: <https://pa1bbexp01.ux.corp.local:9093/#/alerts> Prod Blackbox Exporter URL: <https://pa1bbexp02.ux.corp.local:9115/> Prod Alert Manager URL: <https://pa1bbexp02.ux.corp.local:9093/#/alerts> |
| Grafana (on-premies hosted) | <https://brgraph1.ux.corp.local:3000/> |
| AWS OpenSearch - Dev | <https://vpc-dev-elasticsearchdomain-bjebaegxp5yg3mjcr2r46ni3se.us-west-2.es.amazonaws.com/_dashboards/app/home#/>  To get access to AWS OpenSearch, please submit MyAccess request for entitlement "**Access\_ES-Read-Only\_SSO**"  **Note:** In order to access resources on AWS, user should be part of **FW\_Security-Audit.**Please submit MyAccess request for this entitlement too. |
| AWS OpenSearch - Prod | <https://vpc-prod-elasticsearchdomain-vebniyzt7mbwfmiqdp75p54kmm.us-west-2.es.amazonaws.com/_dashboards/app/home#/>  To get access to AWS OpenSearch, please submit MyAccess request for entitlement "**Access\_ES-Read-Only\_SSO**"  **Note:** In order to access resources on AWS, user should be part of **FW\_Security-Audit.**Please submit MyAccess request for this entitlement too. |
| Oracle Logging Analytics | Oracle Logging Analytics can be accessed from within OCI Console => Main Menu → Observability & Management → Logging Analytics → Log Explorer URL: <https://www.oracle.com/cloud/sign-in.html?tenant=trinetgrp> Cloud Account Name: trinetgrp  Direct Link to Oracle Logging Analytics: <https://cloud.oracle.com/loganalytics/explorer?jobId=c026a2f3-3edb-1f8c-40a4-8bd2b63addde&region=us-phoenix-1>  To get access to Oracle Logging Analytics, please submit [MyAccess](https://myaccess.trinet.com/identityiq/home.jsf) request for entitlement "**OCI SecurityAudit Global**"  Oracle Logging Analytics Brownbag session: [Grafana and Oracle Logging Analytics Brown bag session-20230712\_120425-Meeting Recording.mp4](https://trinethr-my.sharepoint.com/:v:/r/personal/sampath_basireddy_trinet_com/Documents/Recordings/Grafana%20and%20Oracle%20Logging%20Analytics%20Brown%20bag%20session-20230712_120425-Meeting%20Recording.mp4?csf=1&web=1&e=lcQE8s) |
| AppDynamics - Prod | <https://trinet-prod.saas.appdynamics.com/controller/>  Account: trinet-prod  To get access to AppDynamics, please submit MyAccess request for entitlement  "**AppDynamics - Access AppDynamics SSO**" |
| AppDynamics - Test | <https://trinet-test.saas.appdynamics.com/controller/>  Account: trinet-test  To get access to AppDynamics, please submit MyAccess request for entitlement  "**AppDynamics - Access AppDynamics SSO**" |
| ThousandEyes (Digital Experience Monitoring Tool) | <https://app.thousandeyes.com/login>  To get access to Thousand, please submit MyAccess request for entitlement "**ThousandEyes Regular User**" |

Overall this topic explains an Overview of all the Monitoring tools used in PEO, HRIS, DCP applications in TriNet