ForgeRock

Gestion D’acces

Contrôler l’accès des personnes, des services et des objets

Notre démarche en matière de gestion d’accès ? Une seule solution à déployer, pourvu de fonctionnalités complètes permettant de contrôler l’accès à tous les objets de votre monde, physique ou numérique. Plus besoin d’intégrer un ensemble de produits hétérogènes. Les solutions d’identité modernes doivent adopter une approche par plateforme et assurer une interaction plus fluide entre les personnes, les services et les objets, tout en offrant la meilleure sécurité possible. Une plateforme d’identité performante peut aider l’entreprise à transformer l’identité en force motrice pour créer de nouveaux flux de revenus grâce à des produits et des services tant originaux que novateurs.

Pour ce faire, la plateforme d’identité doit permettre une expérience utilisateur dynamique et personnalisée, grâce à des méthodes d’authentification modernes qui vont au-delà du simple nom d’utilisateur avec mot de passe. En effet, une granularité supérieure est nécessaire à l’authentification pour protéger et sécuriser les ressources. La plateforme doit être en mesure de

fournir des services d'identité et d'accès qui soient sécurisés en continu, évolutifs et capables de s'adapter à l'évolution rapide de la demande.

La solution *ForgeRock Access Management*, qui s'intègre à la *ForgeRock Identity Platform*™, fournit l'ensemble le plus complet et le plus souple de services permettant la gestion d'identités et d'accès clients. Elle dispose également de fonctionnalités traditionnelles pour la gestion d'accès. Ces services comprennent l'authentification avancée, l'authentification adaptative, l'authentification intelligente, l'authentification et l'autorisation mobiles en mode « push », l'autorisation contextuelle, la fédération, le Signle-Sign-On, la confidentialité et le consentement, la gestion de session à haute performance et l'architecture OAuth 2.0 Proof-of-Possession.

Caractéristiques et avantages

Authentification avancée et intelligente

Des possibilités d'authentification infinies avec plus de 30 moyens d'authentification prêts à l'emploi et une arborescence d'authentification dont les nœuds permettent de répondre aux besoins spécifiques de l'entreprise.

Mise en œuvre d'une authentification multifactorielle solide.

Création rapide de parcours dynamiques d'authentification du client sur n'importe quelle plateforme.

Analyse poussée des identifiants de connexion pour augmenter le taux d'adoption et améliorer l'expérience utilisateur.

Facilité de configuration et de modification du parcours de connexion en fonction de l'appareil, du contexte, du comportement et du choix de l'utilisateur, et des facteurs de risque.

Repérage automatique des utilisateurs suspects pour une surveillance plus poussée.

Utilisation de moyens d'authentification prêts à l'emploi ou de l'authentification biométrique type FIDO, et intégration à des solutions de cyber-sécurité – de manière centralisée.

A Retenir

- Gestion d'accès "tout-en-un", dans le cadre d'une plateforme d'identité complète.
- Simplicité du paramétrage de l'authentification et de l'autorisation, et souplesse dans la gestion des personnes, des services et des objets.
- Authentification mobile et autorisation en mode « push », notamment par une connexion et validation sans mot de passe ; authentification multifactorielle fluide en mode « push », grâce à une appli mobile conviviale pour iOS et Android.
- Autorisation et authentification de l'identité, avec évaluation continue du contexte en temps réel pour une expérience omni-canal idéale tout au long du parcours de l'utilisateur, par opposition à un processus de décision ponctuelle.
- Architecture souple proposant des modes avec et sans état, conçue pour les exigences de déploiements élastiques à grande échelle comme les environnements DevOps avec micro-services, et l'Internet des Objets (IoT).
- Protection contre le vol de jetons grâce à l'architecture OAuth 2.0 Proof-of-Possession.
- Visualisation et analyse des données de journalisation et d'audit en tout point de la plateforme à l'aide du Framework d'audit commun (CAF) ; prise en charge de la stack Elastic.
- Déploiement dématérialisé ou sur site, notamment via AWS, Azure, etc.

Authentification et autorisation mobiles

Permettre une authentification multifactorielle et une connexion par mot de passe fluides, notamment l'authentification en mode « push » sur les appareils iOS et Android.

Les standards OATH et HOTP permettent d'utiliser un mot de passe à usage unique sur un téléphone portable ou un autre appareil comme facteur d'authentification supplémentaire.

Permettre aux consommateurs d'autoriser de manière sûre et pratique des transactions et des événements à haut risque, par le biais de notifications sur leur téléphone portable.

Authentification adaptative

Exploiter l'authentification contextuelle pour évaluer les risques, en réservant les mécanismes d'authentification renforcée aux cas strictement nécessaires, grâce à une évaluation de l'identité de l'utilisateur et de son contexte.

Autorisation

Autorisation sommaire et précise fondée sur des règles entièrement personnalisables, qui exploitent le contexte et la sécurité en continu pour permettre un accès contrôlé aux ressources grâce à de simples manipulations (pointer-cliquer, glisser-déposer).

Les scripts peuvent être utilisés, pendant l'évaluation des règles, pour étendre la logique à tout type de ressources, non seulement les URL mais aussi les services externes ou les appareils et objets connectés (IoT).

Fédération

Exploiter les normes pour assurer une fédération homogène entre les organisations.

Intégrer la fédération SAML2 dans les chaînes d'authentification, ce qui permet l'usage d'identités fédérées dans des scénarios d'authentification multifactorielle renforcée.

Prendre en charge OpenID Connect, pour faciliter et accélérer la construction de solutions nécessitant des données d'identité supplémentaires.

Identification unique

Fournir des services d'identification unique (SSO) pour des ressources multiples sur un ou plusieurs domaines, ou même plusieurs organisations. Cela permet d'utiliser une seule clé d'authentification pour accéder à toutes les ressources.

Activer un environnement SSO fluide constitué d'applications Web et de systèmes d'exploitation hétérogènes, avec prise en charge de l'identification unique (SSO) par Windows Desktop.

Identification sociale

Accélérer l'accueil des utilisateurs via un fournisseur d'identité (IDP) social prenant en charge OpenID Connect ou OAuth 2.0, comme Facebook, Google, LinkedIn, Instagram, VKontakte, et WeChat.

Gestion des sessions

Une grande souplesse dans la gestion des sessions (avec ou sans état).

La gestion de sessions sans état et les serveurs autonomes permettent des déploiements élastiques hautement distribués avec une extensibilité horizontale presque illimitée.

La gestion de sessions avec état permet aux utilisateurs finaux de disposer en permanence d'environnements complexes et multi-sites avec une disponibilité très élevée.

Services partagés

Le framework d'audit commun (CAF) assure un enregistrement homogène des données en tout point de la plateforme d'identité ForgeRock, et permet la corrélation des événements et des transactions. Les sujets d'audit, tels que l'accès et l'activité, peuvent être configurés de façon indépendante, pour fournir les données souhaitées aux services appropriés. (Comprend des gestionnaires pour les fichiers CSV, les connexions JDBC, Syslog, JMS et Elasticsearch, intégré à la stack ELK).

Les services partagés peuvent enregistrer et suivre les transactions, mais aussi créer des interfaces utilisateur personnalisées, développer des scripts grâce à JavaScript et Groovy, et fournir aux utilisateurs un libre-service sur l'ensemble de la plateforme.

DevOps et assistance aux développeurs

Développement adossé aux API RESTful communes de la plateforme, qui permettent l'utilisation de JSON ou XML via HTTP. Cela permet d'accéder à tous les services sous-jacents d'authentification, d'autorisation et d'identité. Des API Java et C sont également disponibles.

Exploiter l'automatisation et l'orchestration dans un environnement dématérialisé (cloud) pour un déploiement instantané et une mise à disposition en continu, avec prise en charge de Docker et de puissants utilitaires de ligne de commande qui s'intègrent de manière transparente dans les environnements DevOps.

Le service de jetons de sécurité (STS) traduit automatiquement les protocoles pour les fournisseurs qui prennent en charge des normes de fédération et d'authentification différentes.

Performance et évolutivité

Prendre en charge des mises en oeuvre à grande échelle et à haute disponibilité avec des millions d'utilisateurs, des dizaines de milliers de sessions concomitantes et des milliers d'authentifications par seconde.

Exploiter les services d'annuaire intégrés ForgeRock comme référentiel de configuration, et comme référentiel hautement évolutif et performant de jetons et d'utilisateurs persistants au-delà des sessions.

Normes

Tous les principaux protocoles de fédération : SAML 1.x, SAML 2.0 (SP, IdP, ECP, et IdP Proxy), WSFederation (émetteur ou consommateur d'assertions).

Normes de fédération Nouvelle Génération pour un usage mobile et dématérialisé (cloud), y compris la mise en œuvre complète des normes OpenID Connect, OAuth 2.0, GSMA et UMA 2.0, pour une plus grande interopérabilité et une harmonisation du travail des développeurs.

Exportation et importation de règles via XACML.

La solution ForgeRock Access Management fait partie de la ForgeRock Identity Platform, la seule offre conjuguant gestion d'accès, gestion d'identités, accès géré par l'utilisateur, services d'annuaire, sécurité périphérique et passerelle d'identité, qui soit conçue et construite comme une plateforme unique et unifiée. La solution repose sur une architecture hautement évolutive, modulaire, extensible et facile à déployer. Ses capacités contextualisées permettent à vos salariés, clients ou citoyens de vivre une expérience personnalisée sur n'importe quel canal numérique, qu'il s'agisse d'un appareil mobile, d'une voiture connectée, d'un appareil ménager ou de toute autre innovation connectée à venir.

A propos de ForgeRock

ForgeRock, numéro un de l'identité numérique, fournit des solutions modernes et complètes pour la Gestion d'Identité et d'Accès (IAM). Ces solutions permettent aux consommateurs, aux salariés et aux objets d'accéder au monde connecté en toute sécurité et simplicité. Plus d'un millier d'organisations clientes dans le monde ont recours à ForgeRock pour orchestrer, gérer et sécuriser le cycle de vie complet des identités, grâce à un contrôle d'accès dynamique, une gouvernance, des API et un stockage des données maîtresses, qui peuvent être manipulées dans n'importe quel environnement dématérialisé ou hybride. ForgeRock est une société privée dont le siège social se trouve à San Francisco, en Californie, et dispose d'antennes dans le monde entier. Pour de plus amples informations et des téléchargements gratuits, consultez www.forgerock.com ou retrouvez **www.forgerock.com** sur les réseaux sociaux.

Retrouvez nous

ForgeRock