

Mis à jour le 06/10/2026

S'inscrire

Formation Zscaler Private Access (ZPA)

3 jours (21 heures)

Présentation

Zscaler Private Access est une solution ZTNA permettant de sécuriser les accès aux applications privées sans ouvrir le réseau aux utilisateurs. Avec les App Connectors et les politiques contextuelles, ZPA relie chaque utilisateur aux seules applications autorisées selon les principes du Zero Trust et du moindre privilège.

Notre formation Zscaler Private Access (ZPA) vous permettra de maîtriser le déploiement, l'administration et la sécurisation des accès privés. Ce parcours autonome de niveau intermédiaire vous prépare aux situations courantes rencontrées en exploitation.

Vous apprendrez à organiser les Application Segments et les groupes associés, à configurer Client Connector et à intégrer un fournisseur d'identité. Vous construirez des politiques combinant groupes utilisateurs, posture des terminaux et contexte de connexion.

À l'issue de la formation, vous serez en mesure de publier des applications avec Browser Access et de déterminer les usages d'un Private Service Edge dans une architecture résiliente. Vous saurez également préparer une migration progressive du VPN vers ZPA.

Cette formation aborde les diagnostics, les journaux et les bonnes pratiques d'exploitation. Des ateliers pratiques de déploiement, de configuration des accès et de résolution d'incidents vous permettront de fiabiliser vos environnements.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Déployer les App Connectors et vérifier leur disponibilité

- Structurer les Application Segments et leurs groupes pour limiter les accès aux applications autorisées
- Intégrer l'identité et configurer des politiques d'accès contextuelles selon le moindre privilège
- Configurer Client Connector et publier une application avec Browser Access dans un environnement de test
- Définir une architecture avec Private Service Edge et préparer une migration progressive du VPN
- Diagnostiquer et résoudre les incidents d'accès à partir des journaux et des contrôles de connectivité

Public visé

- Administrateur réseau et sécurité
- Administrateur système
- Ingénieur sécurité
- Architecte infrastructure
- Ingénieur support réseau

Pré-requis

- Maîtrise des fondamentaux TCP/IP et de la résolution DNS en environnement professionnel
- Connaissance des accès distants par VPN et des principes de filtrage réseau
- Expérience de l'administration de systèmes Windows ou Linux et de machines virtuelles
- Notions de fédération d'identité avec SAML 2.0 et d'authentification multifacteur

Pré-requis techniques

- Poste Windows 11 avec droits d'installation et navigateur récent
- Connexion Internet stable et possibilité d'installer Zscaler Client Connector
- Accès à un environnement de laboratoire Zscaler Private Access fourni ou préparé pour la formation
- Environnement de lab permettant de manipuler App Connectors, identité et applications privée

Programme de notre formation Zscaler Private Access (ZPA)

[Jour 1 - Matin]

Architecture Zero Trust et préparation du déploiement

- Principes du ZTNA, accès applicatif et différences avec un VPN donnant accès au réseau
- Architecture ZPA, rôles des Public Service Edges, des App Connectors et de Client Connector
- Chemin d'une connexion privée, microtunnels et résolution DNS avec adresses synthétiques
- Préparation du tenant, rôles d'administration et inventaire des applications privées et de leurs dépendances

- Prérequis de déploiement des App Connectors, plateformes, connectivité sortante, DNS et placement réseau
- Atelier pratique : Cartographier une architecture de laboratoire et contrôler les prérequis réseau et DNS avant le déploiement.

[Jour 1 - Après-midi]

Déploiement des connecteurs et segmentation applicative

- Installation et enrôlement des App Connectors, jetons OAuth et clés de provisioning selon la méthode retenue
- Organisation des App Connector Groups, redondance et vérification de la disponibilité des connecteurs
- Définition des Application Segments par noms de domaine, adresses et ports nécessaires
- Association des Server Groups aux groupes de connecteurs et découverte dynamique des serveurs
- Organisation des Segment Groups, granularité de segmentation et maîtrise des recouvrements entre segments
- Atelier pratique : Déployer deux App Connectors, créer leurs groupes et définir les segments de deux applications avec leurs Server Groups.

[Jour 2 - Matin]

Identité et accès depuis les postes utilisateurs

- Intégration du fournisseur d'identité avec SAML 2.0, métadonnées, certificats et attributs utilisateurs
- Provisioning des utilisateurs et groupes avec SCIM, distinction entre synchronisation et authentification
- Installation et enrôlement de Zscaler Client Connector sur les postes de test
- Profils applicatifs, profils de transfert et Client Forwarding Policy pour orienter les demandes vers ZPA
- Premières politiques d'accès par groupe utilisateur et application, validation des autorisations et des refus
- Atelier pratique : Intégrer un fournisseur d'identité de test, enrôler un poste et vérifier les accès de deux profils utilisateurs.

[Jour 2 - Après-midi]

Politiques contextuelles et Browser Access

- Construction de politiques d'accès contextuelles combinant identité, groupes, applications et type de client
- Contrôles de posture des terminaux et critères de réseaux de confiance dans les règles d'accès
- Évaluation des règles du haut vers le bas, première correspondance et sélection du segment applicatif le plus précis

- Application du moindre privilège, réduction des segments trop larges et tests de non-régression
- Publication avec Browser Access, accès web sans agent, domaines, certificats et contraintes de compatibilité applicative
- Atelier pratique : Appliquer une règle de posture, tester les accès autorisés et refusés puis publier une application web avec Browser Access.

[Jour 3 - Matin]

Private Service Edge et migration depuis le VPN

- Usages du Private Service Edge, différences avec les Public Service Edges et responsabilités d'exploitation
- Prérequis de déploiement, dimensionnement, groupes, enrôlement et flux entrants et sortants du Private Service Edge
- Préférence de chemin avec les politiques de redirection, disponibilité et scénarios de repli à valider
- Administration sécurisée des composants, mises à jour et contrôle de la résilience des accès applicatifs
- Migration VPN vers ZPA, inventaire des dépendances, cohorte pilote, coexistence contrôlée et critères de retour arrière
- Atelier pratique : Configurer un Private Service Edge préparé, vérifier le chemin d'accès puis réaliser la bascule pilote d'une application avec test de retour arrière.

[Jour 3 - Après-midi]

Exploitation et résolution des incidents

- Méthode de troubleshooting par étapes, identification du périmètre et reproduction d'un incident
- Lecture des diagnostics d'activité utilisateur, événements de connexion, refus de politique et erreurs applicatives
- Diagnostic des incidents Client Connector, authentification, attributs d'identité et posture du terminal
- Vérification des App Connectors, résolution DNS, ports applicatifs et associations entre segments et groupes
- Collecte des journaux, principes du Log Streaming Service, intégration SIEM et constitution d'un dossier d'escalade
- Atelier pratique : Résoudre des incidents injectés de DNS, de politique et de connecteur, vérifier le rétablissement des accès et documenter les actions correctives.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son

inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.