Tallen SI Formation

Frame IP Formation

MANAGEZ VOTRE SYSTÈME D'INFORMATION

Gestion de projet - Réseaux & Télécom - Sécurité

Téléphonie sur IP - Visioconférence - Système

ÉDITO

Notre mission, vous transmettre notre savoir-faire

Depuis maintenant 7 ans, FrameIP et TallenSI forment des professionnels dans les vastes domaines du système et du réseau.

De nombreuses entreprises nous font confiance pour fournir en permanence à leurs managers et leurs collaborateurs les compétences et connaissances dont ils ont besoin pour évoluer ou faire évoluer leurs projets, et ainsi s'adapter aux nouveaux marchés.

En s'appuyant sur des méthodes pédagogiques qui ont fait leurs preuves, nous vous proposons des formations d'exceptions, axées sur le partage, d'une qualité sure et inégalable. Elles sont menées par nos formateurs experts chacun spécialisé dans un ou plusieurs domaines.

Ce nouveau catalogue vous présente nos formations, chacune étant composée de travaux pratiques ou d'ateliers qui vous permettront d'acquérir rapidement les nouvelles compétences dont vous avez besoin, en fonction de votre niveau. Ainsi, vous pourrez immédiatement appliquer vos nouvelles connaissances à vos projets.

Confiez-nous vos attentes et vos besoins, nous vous apporterons la formation la plus juste pour une efficacité optimale !

L'équipe des formateurs

PRÉSENTATION DE FRAMEIP ET DE TALLENSI

FrameIP et TallenSI sont nées de l'expertise acquise depuis de nombreuses années auprès des grands comptes publics et privés. Issues de deux mondes complémentaires, celui des opérateurs et du système, FrameIP et TallenSI apportent leur retour d'expérience et leurs conseils dans le but de bâtir les infrastructures et solutions de demain en accompagnant leurs clients dans la conception et la réalisation de projets à fortes valeurs ajoutées.

À l'écoute constante de vos besoins et du marché, FrameIP et TallenSI proposent les solutions les plus adaptées à l'environnement de l'entreprise. Rigueur, méthodologie et expertise technique permettent de répondre à des problématiques complexes. Ainsi, les deux sociétés interviennent sur des réseaux nationaux, mais également régionaux.

Centres de formations professionnelles, FrameIP et TallenSI proposent des formations techniques sur mesure, adaptées aux besoins des entreprises, afin de transmettre l'expertise nécessaire à leurs équipes. C'est pour accompagner les entreprises dans cette dynamique que FrameIP et TallenSI proposent un service global de la conception à la réalisation, en passant par la formation des employés.

Les formations sont fondées sur 5 valeurs :

- Le partage
- L'innovation
- Le pragmatisme
- L'expertise
- La qualité

Ces 5 valeurs représentent la philosophie de FrameIP et TallenSI, tant sur les aspects techniques que sur les finitions d'un projet dans sa globalité au niveau de l'offre, des services, de la valeur ajoutée, mais aussi concernant la finalité d'une formation.

Formation en intra-entreprise

Une formation en intra entreprise regroupe les salariés d'une même entreprise dans une même session. Elle peut se dérouler dans les locaux de l'entreprise ou bien dans un centre de formation. Les avantages que peut vous apporter une session de ce type :

- La prise en compte de votre contexte professionnel
- Une confidentialité assurée sur l'activité de votre structure
- Un intérêt financier en formant plusieurs collaborateurs dans une seule session, à partir de 2 personnes
- La possibilité de réaliser un plan de cours spécifique (sur mesure) lié à l'activité de l'entreprise, ou aux besoins des participants

Formation en inter-entreprise

Une formation en inter-entreprise regroupe des salariés de diverses entreprises dans une même session. Elle se déroule exclusivement dans un centre de formation. Les avantages que peut vous apporter une session de ce type :

- Les formations inter-entreprise réunissent des participants d'entreprises différentes. La diversité des entreprises dans lesquelles ils travaillent, enrichit la qualité des échanges et élargit la vision du participant
- L'objectif de nos formations inter-entreprise est d'acquérir les fondamentaux professionnels, les savoir-faire indispensables aux fonctions de chefs de projets entre autres
- Si vous n'avez qu'une ou deux personnes à former, le coût financier est plus avantageux en inter

Frame IP Formation

UNE MÉTHODOLOGIE D'ACCOMPAGNEMENT

EN AMONT

- Évaluation des acquis au démarrage :

Nous vous proposons de réaliser des tests pour évaluer le niveau des participants, votre environnement informatique, vos installations, cadrer les besoins afin d'être en adéquation avec la formation demandée.

- Proposition :

Suite aux résultats des évaluations, un plan de cours, soit dit de «catalogue» pour les formations de base, soit dit «spécifique» ou «sur mesure».

- Envoi des documents :

Des convocations, des conventions et des plans d'accès.

PENDANT

- Vérification des acquis en cours de formation :

À la fin de chaque chapitre de formation, le formateur évalue les acquis et réajuste sa progression pédagogique sur la journée. Cette évaluation permet de mesurer et d'adapter la progression en visant les objectifs pédagogiques et opérationnels définis en amont.

- Évaluation à chaud des participants :

Les participants remplissent un questionnaire pour le Contrôle Qualité de la formation dispensée. Celui-ci porte sur les aspects : organisation, objectif, matériel, pédagogie, technique, résultats.

APRÈS

- À l'issue de la session de formation

Le formateur et le chef de projet procèdent à un bilan de l'action portant sur : le déroulement du stage, la progression individuelle et de groupe des participants, les remarques et suggestions. Ce bilan vous est envoyé une semaine après la session. Ensuite, le chef de projet prend contact avec vous pour en discuter. Une attestation de fin de stage est délivrée à chaque personne ayant suivi la formation.

- Évaluation à distance :

Quelques temps après la formation, nous reprenons contact avec vous pour évaluer l'« opérationnalité » des personnes formées, nous mesurons les résultats et nous vous remontons l'information.

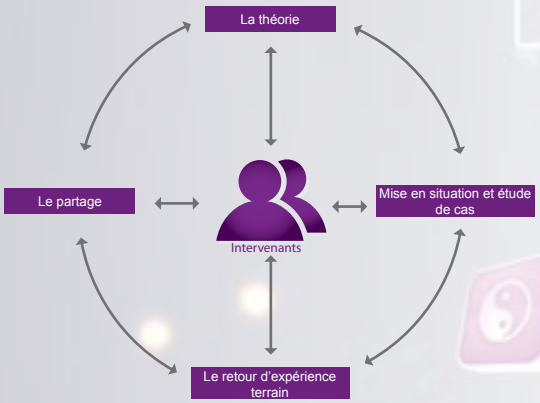
Frame IP Formation

LA PÉDAGOGIE DE FORMATION

La pédagogie est au centre de nos préoccupations. Elle est très importante pour réaliser des formations de qualités. La méthodologie comprend 4 axes indispensables autour du pilier de l'intervenant.

En suivant les différents axes, nos formations suivent un rythme facilitant l'assimilation de l'ensemble des connaissances données :

- La théorie est la base de toute formation. Elle permet d'organiser les différentes briques de connaissance de la formation en question



- La mise en situation ou l'étude de cas met en pratique l'ensemble des compétences acquises lors de la thé briques se mettent alors en place pour une meilleure compréhension de connaissances délivrées. Cette étape peut s'effectuer sur l'ensemble des plans de cours proposés. Cette étape est primordiale dans le processus de formation.

- Le retour d'expérience terrain l'intervenant doit également: faire part de son expérience terrain concernant les différentes problématiques que l'on peut rencontrer surtout en gestion de projet. L'intervenant peut répondre aux questions posées et faire une analyse de la mise en situation précédemment effectuée.

- Le partage est une chose importante pour nous. Il est donc normal que les intervenants conseillent les meilleurs ouvrages et les meilleures adresses Web pour approfondir les connaissances

Enfin, au centre de ces quatre axes, nous trouvons les intervenants : pierres angulaires de la qualité de l'ensemble de la formation. Chez nous, les intervenants sont choisis en fonction de leurs compétences, de leur expérience, mais surtout de leur capacité à restituer l'ensemble de leurs connaissances au public, qu'ils soient débutants ou expérimentés.

TallenSi Formation

Le cycle de la formation reste à l'appréciation de l'intervenant. Ainsi, et suivant le cours que nous vous proposerons, le cycle sera plus ou moins long permettant d'accentuer la formation sur les points les plus critiques.

Il peut donc être envisagé de faire :

- Un cycle court : l'ensemble des étapes se fait sur 1/2 journée
- Un cycle standard : l'ensemble des étapes se fait sur une journée avec la théorie le matin et étape de mise en situation ou étude de cas, de retour d'expérience terrain et de partage l'après-midi
- Un cycle long : l'ensemble des étapes se fait sur plusieurs jours. La théorie est faite au début et les étapes se suivent les jours suivants

GESTION DE PROJET

RÉSEAUX ET TÉLÉCOMS

SÉCURITÉ

COMMUNICATIONS UNIFIÉES

SYSTÈME

GESTION DE PROJET

- GP 101 Initiation à la gouvernance
- GP 102 Conduire un projet informatique
- GP 103 Réaliser son schéma directeur
- GP 104 AMOA d'un projet
- GP 105 ITIL Foundation V3
- GP 106 CMMI
- GP 107 PCA - Initiation et méthodologie
- GP 108 PCA - Construire son PCA
- GP 109 PCA - Audit, analyse et classification des risques
- GP 110 PCA - Composer son référentiel
- GP 111 PCA - Maintien en condition opérationnelle
- GP 112 Élaborer un modèle conceptuel de données avec Merise

Le chef de projet est la personne chargée de mener un projet et de contrôler son bon déroulement. De manière générale, il dirige ou anime une équipe pendant la durée du ou des divers projets dont il a la charge.

Le chef de projet, chez FrameIP et Tallen SI, est l'interlocuteur privilégié du client parmi tous les acteurs du projet. Il gère, assure, garantit et optimise le bon déroulement des projets. Il respecte les stratégies d'entreprise et les schémas directeurs décidés avec le client.

L'impact du chef de projet est majeur pour la réussite du projet. C'est pourquoi, tous nos chefs de projet représentent notre philosophie, tant sur les aspects techniques que sur les finitions d'un projet dans sa globalité au niveau de l'offre, des services, de la valeur ajoutée, mais aussi concernant la finalité d'une formation.

GP 101

INITIATION À LA GOUVERNANCE

OBJECTIFS

Cette formation d'introduction à la gouvernance offre les éléments clés pour mieux comprendre les différentes facettes du SI tant sur le plan économique, organisationnel, humain que technique et ainsi mieux appréhender le mécanisme de fonctionnement et d'évolution de celui-ci.

PUBLIC

Cette formation est orientée pour les directeurs informatiques, les directeurs des systèmes d'information et de façon générale pour les décideurs et acteurs clés du système d'information.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

GOUVERNANCE ET SI

Qu'est-ce que la gouvernance ?
Importance du SI dans la réussite de l'entreprise
Les principes clés
Le coût et la valeur du SI

MISE EN ŒUVRE DE LA GOUVERNANCE

Les outils et référentiels
La gouvernance sur le plan économique
La gouvernance sur le plan organisationnel et humain
La gouvernance sur le plan de la production

LA MAÎTRISE DES COÛTS

L'alignement stratégique
La mesure des coûts du SI
Établir une stratégie de maîtrise des coûts
Construire un budget informatique et le vendre à la Direction Générale
L'organisation et les ressources humaines
La gestion des compétences
L'achat de prestations intellectuelles et l'externalisation
Les méthodes de conception, de conduite et de communication
La gestion des risques et des cas de crise

LA STRATÉGIE TECHNOLOGIQUE ET LA GESTION DES PROJETS

La veille technologique
La maîtrise du déroulement et du suivi des projets
La conduite du changement
Support utilisateur
Tableau de bord

GP 102

CONDUIRE UN PROJET INFORMATIQUE

OBJECTIFS

La réussite d'un projet informatique dépend d'un nombre de facteurs importants, certains sous notre contrôle et d'autres non. L'objectif de cette formation est de vous apporter les bonnes pratiques autant d'un point de vue organisationnel et technique que relationnel afin de pouvoir anticiper et réagir rapidement et ainsi conserver la maîtrise de votre projet.

PUBLIC

Toute personne chargée du pilotage d'un projet informatique.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

S'APPROPRIER LE PROJET

Comprendre le projet et sa finalité
Identifier les différents acteurs et leurs rôles
Distinguer les différents besoins et contraintes
Discerner les particularités et les difficultés

ESTIMER LE PROJET

Comprendre l'intérêt du découpage en tâches élémentaires
Choisir le cycle de vie adapté au projet
Estimation des délais et des charges
Évaluer les risques liés au projet

PLANIFICATION ET SUIVI

Ordonnancer les tâches
Les outils de planification et de suivi
Gérer les ressources humaines
Validation et clôture du projet

GÉRER LE RELATIONNEL

Les différents types d'interlocuteurs
Apprendre à gérer les situations délicates
Utiliser les vecteurs de communication adaptés
Les réunions

GÉRER LA QUALITÉ

Le rôle de la qualité
Le Plan d'Assurance Qualité
Les normes

GP 103

RÉALISER SON SCHÉMA DIRECTEUR

OBJECTIFS

Le schéma directeur est un outil de planification stratégique du système d'information et celui-ci doit être adapté aux problématiques rencontrées. Cette formation vous offre les méthodologies et les points essentiels pour élaborer votre schéma directeur de A à Z.

PUBLIC

Cette formation est accessible à toute personne étant amenée à travailler de près ou de loin à l'élaboration d'un schéma directeur.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

LE RÔLE DU SCHÉMA DIRECTEUR POUR LE SI

- Intérêt du schéma directeur et stratégie
- Les différents types de schéma directeur : SI, informatique, stratégique
- L'alignement stratégique
- Les principes clés
- Les outils de planification

L'OUTIL DE PLANIFICATION

- Le périmètre
- Les domaines prioritaires
- Les ressources nécessaires et disponibles
- La granularité du schéma directeur

LES MÉTHODES D'ÉLABORATION D'UN SCHÉMA DIRECTEUR

- L'origine des méthodes
- Présentation des différentes méthodes
- Comparaisons : forces, faiblesses, domaines d'application

L'ÉLABORATION DU SCHÉMA DIRECTEUR

- Les étapes de l'élaboration
- Les outils à disposition pour les différentes phases
- Organisation et responsabilité
- Analyse de plans types de schémas directeurs

LA MISE EN OEUVRE DU SCHÉMA DIRECTEUR

- Les scénarios de mise en oeuvre
- Les principales causes d'échec
- Les bonnes pratiques pour réussir sa gestion du changement

GP 104

AMOA D'UN PROJET

OBJECTIFS

Cette formation dresse un État de l'Art de la maîtrise d'ouvrage. Vous apprendrez comment réussir une maîtrise d'ouvrage afin de profesionnaliser votre entreprise.

PUBLIC

Toute personne voulant apprendre les bases de la gestion de projet ou souhaitant renfoncer ses connaissances.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

ORGANISER UNE MAÎTRISE D'OUVRAGE

- Qu'est-ce qu'une maîtrise d'ouvrage : organisation et rôles
- La prise de décision : comité de pilotage et key users
- Apprendre à déléguer sa maîtrise d'ouvrage
- Mettre en place un plan de communication

ÉTABLIR UN CAHIER DES CHARGES

- Rappels sur le cahier des charges
- Les outils de l'expression des besoins (groupes de travail, UML...)

LES CONTRATS DE MAÎTRISE D'OEUVRE

- Les éléments clés d'un contrat
- Maîtriser les phases d'appel d'offre et de négociation
- La gestion de la relation contractuelle

PILOTER UNE RÉALISATION

- Les règles de la conduite des phases de réalisation
- Les rapports avec le maître d'oeuvre interne
- Définir un plan de tests
- Écrire un cahier de recette

METTRE EN SERVICE LE SYSTÈME D'INFORMATION

- Le déploiement sur site
- Site pilote
- Passage en exploitation
- La migration des données
- La conduite du changement
- Support utilisateur
- Tableau de bord

GP 105

ITIL FOUNDATION V3

OBJECTIFS

L'objectif de cette formation est de permettre aux managers, chefs d'équipe et autres d'assimiler les concepts décrits dans la version 3 de l'ITIL. Cette formation constituera une base solide pour l'obtention de la certification ITIL.

PUBLIC

Managers, chefs d'équipes, responsables ou directeurs informatiques.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

PRÉSENTATION DE L'ITIL : INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

- Histoire de l'ITIL : de sa naissance jusqu'à aujourd'hui
- La philosophie de l'ITIL (Best practises)
- La place de l'ITIL dans le «monde» des certifications

LA GESTION DE SERVICE

- Importance de la gestion de service
- ITIL et les autres référentiels qualité
- Impact de l'ITIL sur le SI

LA MAÎTRISE DU CYCLE DE VIE DES SERVICES

- Stratégie des services
- Conception des services
- Transition des services
- Exploitation des services
- Amélioration continue des services

MISE EN OEUVRE AU SEIN DU SI

- Contraintes spécifiques
- Les facteurs clés du succès
- Organisation et planification de la mise en oeuvre
- Notre retour d'expérience sur le sujet

PRÉPARATION À LA CERTIFICATION

- Apprendre à «parler» ITIL
- Gérer son temps à l'examen
- Notre retour d'expérience : les pièges à éviter

TP : EXAMEN BLANC

GP 106

CMMI

OBJECTIFS

Dans la stratégie de l'entreprise, le système d'information doit démontrer son efficacité afin de s'inscrire dans la stratégie de l'entreprise. CMMI répond à ses problématiques grâce à un référentiel reconnu au niveau international. Grâce à ce cours, les participants vont acquérir des bases solides dans ce référentiel.

PUBLIC

Débutant

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

CONCEPT DE BASE

- Qu'est-ce que CMMI ?
- Les enjeux d'un modèle de processus
- Les différences avec les autres modèles
- L'intérêt de la mise en place du modèle pour l'entreprise
- L'intérêt de la mise en place du modèle pour les clients
- Les concepts clés

LE CONTENU CMMI

- L'architecture du modèle de maturité
- Les processus
- Structure du modèle à étages

LES FONDEMENTS DE LA MISE EN OEUVRE

- Diagnostic CMMI
- Cycle de suivi et d'amélioration des processus
- L'évaluation de la maturité

LA CERTIFICATION

- Évaluer son niveau

ÉTUDES DE CAS : UN EXEMPLE DE MISE EN OEUVRE

GP 107

PCA - INITIATION ET MÉTHODOLOGIE

OBJECTIFS

La mise en place d'un plan de continuité d'activité requiert avant tout une connaissance théorique sur le sujet ainsi que de l'organisation et de la méthodologie. L'objectif étant d'offrir aux participants des bases solides dans ce domaine.

PUBLIC

Débutant souhaitant acquérir les bases du domaine.

1 JOUR

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION AU PCA

Les principales définitions
Le contexte PCA en entreprise
Les objectifs

LES ENJEUX POUR L'ENTREPRISE

Les enjeux de la continuité de service
Les concepts clés
Les contraintes réglementaires devenues exigences (Assurances, norme Bâle II, recommandation ISO)

LES FONDAMENTAUX

Les différents aspects du PCA
Le développement d'une stratégie de continuité
L'analyse d'impact sur l'activité
Composer son référentiel
Maintien en condition opérationnelle

LA MÉTHODOLOGIE

Les principales étapes de la méthodologie
De la prise de conscience à la classification du SI
Les prémices de la mise en place d'un PCA
Mise en place du PCA en entreprise

NORMES ET BONNES PRATIQUES

Les différents acteurs
Niveau international
La situation en France

GP 108

PCA - CONTRUIRE SON PCA

OBJECTIFS

Un grand nombre d'entreprises ne survivrait pas à une interruption de leur système d'information. Bien plus qu'une assurance vie, le plan de continuité d'activité permet à l'entreprise d'être efficace face aux sinistres et d'opter pour une organisation optimisée.

PUBLIC

Débutant

3 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

LE PLAN DE CONTINUITÉ

Retour sur la méthodologie
Les différentes phases du PCA
Les objectifs

PHASE 0 : SENSIBILISER LA DIRECTION

Les enjeux
La méthodologie

PHASE 1 : L'ANALYSE DES RISQUES

L'analyse des services
L'analyse des risques
L'analyse d'impacts
Développement de la stratégie de continuité

PHASE 2 : L'ÉLABORATION DU PCA

Définir les missions et les responsables
La politique de continuité et le référentiel PCA
Mise en place des plans (Plan de secours, plan d'hébergement externe, plan de communication...)
Planifier le PCA
Le PCA et la gestion de projet
L'ingénierie de la continuité (construire la disponibilité, gérer la continuité informatique)
Valider le plan de continuité

PHASE 3 : MAINTIEN EN CONDITION OPÉRATIONNELLE

Redéfinition du MCO
Le système de contrôle
Test du PCA et optimisation

ÉTUDE DE CAS ET ATELIER

GP 109

PCA - AUDIT, ANALYSE ET CLASSIFICATION DES RISQUES

OBJECTIFS

Dans la méthodologie de plan de continuité, un des composants réside dans les risques. En amont du projet, l'analyse et la classification des risques permettront à l'entreprise de connaître les menaces auxquelles elle est exposée et l'impact sur l'entreprise. Les actions découlant de l'analyse feront partie du référentiel final ainsi que les options permettant de réduire les effets.

PUBLIC

Débutant ou intermédiaire

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION AUX RISQUES

- Définitions des risques
- Les prérequis à l'analyse des risques
- Appréciation des risques
- Le traitement des risques
- Prise de décision face aux risques

L'ANALYSE DES BESOINS EN SÉCURITÉ

- Identification des services critiques
- Classification des services
- Les différentes bases d'objectifs (temps de reprise (RTO), point de reprise (RPO)

L'ANALYSE DE L'IMPACT D'UN RISQUE SUR L'ENTREPRISE

- Chronologie d'un sinistre
- Corrélation entre risque, sinistre et impact
- Les composants de l'analyse d'impact
- Établir le document d'analyse d'impact

DÉTERMINER LA STRATÉGIE DE CONTINUITÉ

- Corrélation des risques et des besoins en termes de reprise
- Corrélation des risques et des besoins en termes de continuité
- Communiquer la stratégie de continuité auprès des métiers
- Étude de faisabilité
- Établir le document de stratégie de continuité

MÉTHODOLOGIE D'ANALYSE DES RISQUES

- L'objectif des méthodologies
- Mehari : analyse des risques
- Ebios : expression des besoins en termes de sécurité informatique
- Méthodologie annexe

ÉTUDE DE CAS : MISE EN PLACE D'UNE ANALYSE DE RISQUE

GP 110

PCA - COMPOSER SON RÉFÉRENTIEL

OBJECTIFS

Dans un plan de continuité, un document doit centraliser l'ensemble des informations. Ce document est le référentiel PCA. Grâce à ce cours, les participants vont acquérir les connaissances nécessaires à la création du référentiel ainsi qu'à la définition de son contenu.

PUBLIC

Débutant, chef de projet, DSI et RSI

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION AU RÉFÉRENTIEL

- Objectif du référentiel
- Les enjeux du référentiel
- Les différentes parties du référentiel
- Les bonnes pratiques

LE CONTENU DU RÉFÉRENTIEL

- Les définitions
- La politique de continuité
- Le système d'information
- Composition du référentiel
- Étude des besoins et des risques
- Le catalogue de procédure

LES PROCESSUS DU PCA

- Les solutions techniques et organisationnelles
- Planning général des opérations
- Le centre de gestion de crise
- Le plan de communication

ÉTUDE D'UN RÉFÉRENTIEL PCA

GP 111

PCA - MAINTIEN EN CONDITION OPÉRATIONNELLE

OBJECTIFS

Aussi important que la mise en place d'un PCA, le maintien en condition opérationnelle est primordial pour l'entreprise. Grâce à ce cours, les participants seront en mesure de maintenir le PCA actif et de protéger l'activité de l'entreprise.

PUBLIC

Débutant ou intermédiaire

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

LE MAINTIEN EN CONDITION OPÉRATIONNELLE

- Retour sur la politique de continuité
- Formation et sensibilisation
- Les tests et la prise en compte des conclusions
- Les concepts clés
- La mise en place des procédures
- MCO et PDCA

LE SYSTÈME DE CONTRÔLE

- Les objectifs et l'importance des tests
- Les différents niveaux de tests
- Les points de vérification des déroulements des tests
- L'évaluation des différents plans PCA
- Mise à jour du PCA
- Un perpétuel recommencement
- Programmation de revues régulières

TESTER LE PLAN DE CONTINUITÉ

- Cadrer un test
- Faut-il annoncer le test?
- Élaborer un plan de test
- Les différentes phases de l'élaboration du plan
- Exécuter le test
- Tirer parti des conclusions

EXEMPLE DE CONCEPTS MCO

GP 112

ÉLABORER UN MODÈLE CONCEPTUEL DE DONNÉES AVEC MERISE

OBJECTIFS

- Aborder un cas concret de modélisation d'application avec Merise
- Savoir optimiser les applications via la séparation des traitements et des données
- Acquérir des techniques de modélisation d'une base de données en garantissant son intégrité
- Savoir utiliser un outil du marché

PUBLIC

Analystes, développeurs, concepteurs et chefs de projets

PRÉREQUIS

Connaissances de base en informatique. Il est nécessaire de disposer d'une culture générale sur le champ des bases de données

3 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

HISTORIQUE

APPROCHE MERISE

- Cycle de vie projet
- Cycle de décision et d'abstraction

PRÉSENTATION ET POSITIONNEMENT DES MODÈLES MERISE

- Modèles conceptuels, physiques, logiques et organisationnels

MODÈLE CONCEPTUEL DE COMMUNICATION (MCC)

- Acteurs internes et externes
- Flux d'informations échangés
- Validation du modèle

MODÈLE CONCEPTUEL DE DONNÉES (MCD)

- Domaines et règles de gestion
- Informations et entités
- Propriétés d'entités et identifiants d'entités
- Association entre entités
- Définition des cardinalités

MODÈLE CONCEPTUEL DE TRAITEMENT (MCT)

- Analyse des flux
- Définition des opérations, des règles d'émission

MODÈLE PHYSIQUE DE DONNÉES (MPD)

- Mise en oeuvre avec génération MCD vers MPD
- Dé-normalisation d'un MPD

MODÈLE ORGANISATIONNEL DE TRAITEMENTS (MOT)

- Procédures et acteurs
- Identification des phases et leurs événements
- Définition des attributs des phases

Frame IP Formation

Tallen Si Formation

RÉSEAUX ET TÉLÉCOMS

- RES 201 Introduction aux réseaux
- RES 202 Introduction aux routeurs
- RES 203 Introduction aux télécommunications
- RES 204 Introduction aux WiFi
- RES 205 Les routeurs - Niveau avancé
- RES 206 Les réseaux sans fil
- RES 207 Les réseaux
- RES 208 Administration et configuration d'un réseau
- RES 209 Administrateur réseau Cisco certifié CCNA ICND1
- RES 210 Administrateur réseau Cisco certifié CCNA ICND2
- RES 211 Comment architecturer un réseau ?
- RES 212 Comment exploiter un réseau ?
- RES 213 Administrer avec Cisco ACS 5.0
- RES 214 Administration avec Ciscoworks LMS 4.0
- RES 215 État de l'Art Ciscoworks LMS 3.2
- RES 216 Mettre en oeuvre la QoS LAN Cisco
- RES 217 Configurer et administrer des Switch HP
- RES 218 Configuration des services réseaux TCP / IP
- RES 219 Superviser son réseau avec Nagios

Un réseau de communication peut être défini comme l'ensemble des ressources matérielles et logicielles liées à la transmission et l'échange d'information entre différentes entités. Suivant leur organisation, ou architecture, les distances, les vitesses de transmission et la nature des informations transmises, les réseaux font l'objet d'un certain nombre de spécifications et de normes.

La connaissance approfondie des réseaux et des équipements permet à nos experts de couvrir l'ensemble des domaines tels que l'administration et la configuration, la supervision mais aussi la télécommunication.

RES 201

INTRODUCTION AUX RÉSEAUX

OBJECTIFS

Cette formation présente les principes de base des réseaux dans un milieu professionnel.

PUBLIC

Administrateur réseau, technicien réseau.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION

- Définition
- Historique
- Les problématiques
- L'évolution
- Les réseaux

LE MODÈLE OSI

- Couche physique
- Couche liaison de données
- Couche réseau
- Couche transport
- Couche session
- Couche présentation
- Couche application

LE MODÈLE TCP / IP

- Couche application
- Couche transport
- Couche internet
- Couche hôte-réseau

LES MÉDIAS PHYSIQUES

- Paire torsadée
- Fibre optique
- Sans fils
- Les lasers
- Autres

L'ADRESSSAGE

- Adresses MAC
- Adresses IPv4
- Adresses de sous réseau et VLSM
- Adresses IPv6
- TP : segmenter un réseau

LES ÉQUIPEMENTS

- Les concentrateurs
- Les commutateurs
- Les routeurs
- Les pare-feux
- Démo : différence entre les concentrateurs et les commutateurs

LES TOPOLOGIES

- Topologie en étoile
- Topologie en bus
- Topologie en anneau
- Topologie maillée
- TP : mise en oeuvre d'un réseau complet (commutateurs + routeurs)

RES 202

INTRODUCTION AUX ROUTEURS

OBJECTIFS

Cette formation présente les routeurs ainsi que les protocoles de routage. Une formation pratique sera proposée à chaque fin de module.

PUBLIC

Administrateur, technicien

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION

- Les objectifs du cours
- L'intérêt des routeurs
- Présentation des équipements

PRÉSENTATION DU ROUTAGE

- Le routage statique
- Les protocoles de routage dynamique
- La convergence
- La distance administrative
- TP : mise en oeuvre des routes statiques

LE PROTOCOLE RIP

- Présentation du protocole RIP
- Principe de fonctionnement
- Les versions
- Avantages / inconvénients
- TP 1 : mise en oeuvre du protocole RIPv1
- TP 2 : mise en oeuvre du protocole RIPv2

LE PROTOCOLE EIGRP

- Présentation du protocole EIGRP
- Principe de fonctionnement
- L'algorithme DUAL
- Avantages / inconvénients
- TP : mise en oeuvre du protocole EIGRP

LE PROTOCOLE OSPF

- Présentation du protocole OSPF
- Principe de fonctionnement
- L'algorithme SPF
- Avantage / inconvénients
- TP : mise en oeuvre du protocole OSPF

RES 203

INTRODUCTION AUX TÉLÉCOMMUNICATIONS

OBJECTIFS

Cette formation présente les principes des Télécommunications d'entreprise et du vocabulaire associé. Elle décrit les normes utilisées en téléphonie, les principes d'architecture, les équipements, les services et les applications disponibles et montre comment structurer et organiser un réseau de téléphonie d'entreprise.

PUBLIC

Ce cours s'adresse à tous les métiers de l'entreprise susceptibles de participer de près ou de loin à l'évolution de la filière téléphonique, que ce soit du personnel technique ou des métiers directement liés à l'activité de l'entreprise. Ce cours peut fournir un excellent prérequis pour les cours de Téléphonie sur IP.

2 JOURS

POINTS CLÉS DU PROGRAMME

RÉSEAUX TÉLÉPHONIQUES

- De la voix à la téléphonie
- Le traitement du signal
- Historique des réseaux téléphoniques RTC, RNIS
- Organisation des réseaux opérateurs
- Les accès opérateurs numériques
- Les signalisations D (Q931), SS7
- Les services évolués et le réseau intelligent
- Évolution des Télécoms

TÉLÉPHONIE D'ENTREPRISE : DU PABX À L'IP CENTREX

- Architecture et composants
- Le traitement des appels
- Le routage et la commutation
- Évolution de l'architecture des réseaux d'entreprise, convergence voix / donnée
- Évolution vers la téléphonie sur IP
- Interconnexion de PABX (RPIS)
- Les Call Centers : architecture et composants
- Les étapes de traitement d'un appel client
- Distribution et gestion de file d'attente
- CTI et les standards CSTA

LA SIGNALISATION

- Rôles et objectifs
- Types de signalisation
- Les standards et la convergence vers l'IP
- Les protocoles multimédias H323, SIP, RTP, MGCP
- Les codecs multimédias (G7xx, AMR, H263, MPEG4)
- Architecture et dynamique des flux

SERVICES ET APPLICATIONS DE LA TÉLÉPHONIE

- Les services de base (double appel, multiligne)
- Les services d'accueil (prédécroché, groupement...)
- Messagerie vocale et messagerie unifiée
- Synthèse vocale et technologie «text to speech»
- Standard automatique et serveur vocal interactif
- Les applications de gestion

LA TÉLÉPHONIE SUR IP

- Besoins des réseaux data et réseau de téléphonie
- Les nouveaux services
- Les scénarios d'entreprise

TÉLÉPHONIE SANS FIL ET TÉLÉPHONIE MOBILE

- Les réseaux mobiles GSM, EDGE et UMTS
- La mobilité sur IP
- La convergence fixe mobile (UMA)

LES SERVICES DE COMMUNICATIONS AVANCÉS

- Personal Information Management
- Services voix / vidéo temps réel via le Web
- Nouveaux services
- Perspectives d'évolution IMS : tendances et opportunités
- Nouveaux usages et conduite du changement

RES 204

INTRODUCTION AU WIFI

OBJECTIFS

Cette formation est une introduction au WiFi qui présente donc la structure de base. Elle touche différents domaines liés au WiFi comme la sécurité et la Vo WiFi.

PUBLIC

Administrateur

4 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION

- Définition et historique
- Les risques et les réglementations
- Les technologies sans fil
- Les réseaux sans fil

PRINCIPES FONDAMENTAUX

- Les ondes électromagnétiques
- La propagation des ondes
- Les fréquences et les canaux
- Les perturbations
- Les SSID
- Les normes
- L'encapsulation
- TP : Configurer un AP et analyser la propagation des ondes

LES INFRASTRUCTURES

- Généralités et concepts
- Le matériel
- Le mode « infrastructure »
- Le mode « Ad-hoc »
- Architecture centralisée
- Architecture distribuée
- TP : configurer un contrôleur WiFi

LA SÉCURITÉ

- Généralités et concepts
- Protocole d'authentification WEP
- Protocole d'authentification WAP-2
- Protocole de chiffrement TKIP
- Protocole de chiffrement AES
- Méthode de filtrage
- TP : Craquer une clé WEP

LA VoWIFI

- Généralité et concepts
- Les normes
- La sécurité
- La QoS et la VoWiFi
- TP : configurer un AP et tester avec un téléphone WiFi

RES 205

LES ROUTEURS - NIVEAU AVANCÉ

OBJECTIFS

Ce cours de perfectionnement vous apportera des connaissances complètes sur les protocoles de routage utilisés par les routeurs CISCO. Les participants aborderont ainsi le routage RIP, OSPF, mais également EIGRP ou encore BGP. Cette formation fera également un point sur la QoS et la gestion des flux, ainsi que sur la sécurité. Nous verrons la tolérance aux pannes avec notamment le protocole HSRP.

PUBLIC

La formation s'adresse aux administrateurs réseau ayant déjà une expérience du routage et notamment sur du matériel CISCO.

PRÉREQUIS

Pour aborder ce stage, les participants doivent maîtriser la gestion des adresses IP. Il est nécessaire de posséder de bonnes connaissances de TCP / IP, ainsi que des bases de configuration des routeurs CISCO.

3 JOURS

POINTS CLÉS DU PROGRAMME

ARCHITECTURE DES RÉSEAUX ROUTÉS

- Rappels nécessaires au niveau de l'adressage IP des routeurs CISCO (Classe, VLSM, CIDR, …)
- Les différentes possibilités de routage

LE ROUTAGE DYNAMIQUE

RIP
- Les versions de RIP
- Le fonctionnement

EIGRP
- Topologie de réseau EIGRP
- Configuration d'EIGRP

OSPF
- Configuration OSPF avancé

BGP
- AS de transit
- Sélection de routes et filtrage

QOS

- Rappels
- Les fonctions de QoS

VPN

- MPLS
- IPSEC

LES ACLS
- Introduction à la sécurité
- Les ACLs simples
- Les ACLs étendues

RES 206

LES RÉSEAUX SANS FIL

OBJECTIFS

Le monde des réseaux sans fil s'enrichit rapidement de nouvelles normes et de nouveaux standards. Ces réseaux permettent de connecter entre eux les équipements de l'entreprise de type voix, données, images. Ils sont également à la base des « hot spots » des opérateurs. Les réseaux IEEE 802.11 (Wi-Fi et toutes les déclinaisons), Bluetooth, UWB, Zigbee, IEEE 802.16, WiMAX, WRAN, etc., seront étudiés en détail dans cette formation ainsi que les applications qui peuvent y être associées. Compte tenu des spécificités et de l'importance de la sécurité, la dernière journée y sera entièrement consacrée.

PUBLIC

Informaticiens et ingénieurs réseaux souhaitant se spécialiser dans les réseaux cellulaires, responsables réseaux mobiles et responsables d'études désireux d'acquérir des connaissances plus approfondies sur le sujet.

PRÉREQUIS

Bonnes connaissances dans le domaine des réseaux d'entreprise

2 JOURS

POINTS CLÉS DU PROGRAMME

PRINCIPES DES RÉSEAUX SANS FIL

- Introduction aux réseaux sans fil
- L'intégration des réseaux sans fil dans l'entreprise
- Les «hot spots» des opérateurs
- Les handovers

BLUETOOTH, UWB, ZIGBEE ET IEEE 802.15

- Les normes IEEE 802.15 et les technologies UWB, Zigbee et Bluetooth
- Le soutien des industriels
- La technologie IEEE 802.15.1 et Bluetooth
- IEEE 802.15.3. La technologie à très haut débit UWB
- Le consortium Wimedia et WUSB
- IEEE 802.15.4 et les produits ZigBee
- Les technologies de réseaux personnels

WIFI IEEE 802.11

- WiFi (IEEE 802.11b/g)
- Mise en place d'un réseau Wi-Fi

LES RÉSEAUX MESH ET LES RÉSEAUX AD-HOC

- Les autres solutions
- Les protocoles et les applications des réseaux sans fil
- L'Internet ambiant
- 3G vs WLAN
- Sécurité WiFi
- Interconnexion des LAN et des WLAN

RES 207

LES RÉSEAUX

OBJECTIFS

Cette formation vous présentera les stratégies de la convergence des réseaux fixes et des réseaux mobiles. Vous verrez également les apports des communications optiques et filaires en termes de convergence ainsi que les interactions entre réseaux existants et évolutions futures.

PUBLIC

Responsables réseaux, responsables études, responsables SI, chefs de projets, architectes réseaux, ingénieurs systèmes et réseaux.

PRÉREQUIS

Bonnes connaissances dans le domaine des réseaux

1 JOUR

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

LES RÉSEAUX

- D'accès terrestres
- D'accès sans fil
- De domicile
- D'accès pour les mobiles

LA CONVERGENCE

- Des réseaux d'accès
- Des réseaux coeurs
- L'intégration dans Internet
- Du réseau de domicile
- Interne aux réseaux mobiles
- Fixe mobile L'IMS
- Les normes
- Les technologies

DIVERS

- Les techniques optiques
- L'introduction d'IP dans la gestion de la mobilité
- Les solutions multiplay
- Le NGN (Next Generation Network)

PERSPECTIVES ET CONCLUSION

RES 208

ADMINISTRATION ET CONFIGURATION D'UN RÉSEAU

OBJECTIFS

Cette formation présente l'essentiel pour administrer et configurer des équipements réseaux Cisco. Une journée sur site peut être envisageable pour une mise en pratique dans l'environnement du client.

PUBLIC

Administrateur

5 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION

- Concepts d'administration et de configuration réseau
- Méthodologie

CONFIGURATION D'UN COMMUTATEUR DE NIVEAU II

- Mise à jour de l'IOS
- Configuration globale
- Configuration de l'administration
- Configuration des VLAN
- Configuration du VTP en mode client
- Configuration du STP
- Mise en place d'une stratégie de sécurité
- Synthèse

CONFIGURATION D'UN COMMUTATEUR DE NIVEAU III

- Mise à jour de l'IOS
- Configuration globale
- Configuration de l'administration
- Configuration des VLAN
- Configuration du VTP en mode serveur
- Configuration du STP en mode root
- Configuration du routage inter-VLAN
- Configuration des ACL
- Mise en place d'une stratégie de sécurité
- Synthèse

CONFIGURATION D'UN PARE-FEU

- Mise à jour de l'IOS
- Configuration globale
- Configuration de l'administration
- Configuration des VLAN
- Configuration des interfaces
- Configuration du routage
- Configuration d'une liaison VPN site à site
- Configuration de liaisons VPN nomades
- Configuration des ACL
- Synthèse

CONFIGURATION D'UN ROUTEUR

- Mise à jour de l'IOS
- Configuration globale
- Configuration de l'administration
- Configuration des VLAN
- Configuration des interfaces
- Configuration du protocole de routage
- Configuration du NAT
- Configuration d'une liaison VPN site à site
- Configuration de liaisons VPN nomades
- Configuration des ACL
- Synthèse

ADMINISTRATION

- Modification du paramétrage global
- Mise à niveau d'un équipement
- Modification des règles de filtrage
- Modification des comptes VPN
- Modification des règles de NAT
- Modification des groupes, objets de sécurité
- Changement d'adresse IP
- Mise à jour des profils d'accès distant
- Synthèse

MAINTENANCE

- Vérification des problèmes liés à une interface
- Vérification des performances d'un équipement
- Contrôle des BPDU sur les interfaces d'accès

RES 209

ADMINISTRATEUR RÉSEAU CISCO CERTIFIÉ CCNA ICND 1

OBJECTIFS

Acquérir l'ensemble des connaissances et la reconnaissance sur les réseaux, l'installation, la configuration et la gestion des routeurs Cisco ainsi que la gestion des switchs Cisco dans le but de passer la certification officielle Cisco Certified Networking Associates (CCNA).

PUBLIC

Techniciens et administrateurs réseaux et technicien support.

4 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

1ER MODULE : LAN SWITCHING

Présentation du test, de la démarche tutorale et du plan de cours
Présentation du chapitre 1

2ÈME MODULE : LANSWITCHING

Questions-Réponses chapitre 1 - Révision
Présentation du chapitre 2

3ÈME MODULE : LAN SWITCHING

Questions-Réponses chapitre 2 - Révision
Présentation du chapitre 3

4ÈME MODULE : TCP/IP

Questions-Réponses chapitre 3 - Révision
Présentation du chapitre 4

5ÈME MODULE : TCP/IP

Questions-Réponses - chapitre 4 - Révision
Présentation du chapitre 5

6ÈME MODULE : TCP/IP

Questions-Réponses chapitre 4 et 5- Révision
Présentation des chapitres 6 et 7

7ÈME MODULE : TCP/IP

Questions-Réponses chapitre 6 et 7 - Révision
Présentation du chapitre 8

8ÈME MODULE : RÉSEAUX LONGUE DISTANCE (WAN)

Questions-Réponses chapitre 8 - Révision
Présentation du chapitre 9

9ÈME MODULE : SÉCURITÉ DES RÉSEAUX

Questions-Réponses chapitre 9 - Révision
Présentation du chapitre 10

10ÈME MODULE : SÉCURITÉ DES RÉSEAUX

Questions-Réponses chapitre 10 - Révision
Présentation du chapitre 11

11ÈME MODULE : SÉCURITÉ DES RÉSEAUX

Questions-Réponses chapitre 11 - Révision
Présentation du chapitre 12

12ÈME MODULE

Test intermédiaire : 30 min – 20 questions
Correction

13ÈME MODULE

Révision de l'ensemble des chapitres
Questions – Réponses

14ÈME MODULE

Révision de l'ensemble des chapitres
Questions – Réponses

15ÈME MODULE :

Test final : 2h – 60 questions

RES 210

ADMINISTRATEUR RÉSEAU CISCO CERTIFIÉ CCNA ICND 2

OBJECTIFS

Acquérir l'ensemble des connaissances et la reconnaissance sur les réseaux, l'installation, la configuration et la gestion des routeurs Cisco ainsi que la gestion des switchs Cisco dans le but de passer la certification officielle Cisco Certified Networking Associates (CCNA).

PUBLIC

Techniciens et administrateurs réseaux et technicien support.

PRÉREQUIS

Maîtrise des consepts de base du réseau (ICND 1)

3 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

1ER MODULE : LAN SWITCHING

Présentation du test, de la démarche tutorale et du plan de cours
Présentation du chapitre 1

2ÈME MODULE : LAN SWITCHING

Questions-Réponses chapitre 1 - Révision
Présentation des chapitres 2 et 3

3ÈME MODULE : TCP / IP

Questions-Réponses chapitres 2 et 3 - Révision
Présentation des chapitres 4 et 5

4ÈME MODULE : TCP / IP

Questions-Réponses chapitres 4 et 5 - Révision
Présentation du chapitre 6 et 7

5ÈME MODULE : TCP/IP

Questions-Réponses - Chapitres 6 et 7 - Révision
Présentation du chapitre 8

6ÈME MODULE : RÉSEAUX LONGUE DISTANCE (WAN)

Questions-Réponses
Chapitre 8 - Révision
Présentation chapitres 9 et 10

7ÈME MODULE : SÉCURITÉ DES RÉSEAUX

Questions-Réponses
Chapitres 9 et 10 - Révision
Présentation chapitres 11 et 12

8ÈME MODULE

Test intermédiaire : 30 min – 20 questions
Correction

9ÈME MODULE :

Révision de l'ensemble des chapitres
Questions – Réponses

10ÈME MODULE

Test final : 2h – 60 questions

RES 211

COMMENT ARCHITECTURER UN RÉSEAU ?

OBJECTIFS

Constituer un réseau local et les systèmes d'exploitation. Comprendre les différentes technologies et problématiques d'entreprise liées au système d'information.

PUBLIC

Techniciens, futurs administrateurs réseau.

4 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

LE MODÈLE DE COMMUNICATION
- Le modèle OSI
- Rôle des différentes couches du modèle OSI
- Autres modèles

TRANSMISSION DES DONNÉES
- Câblage
- Modes de transmission
- Composants réseau
- Postes clients
- Équipements actifs

PRÉSENTATION DES SYSTÈMES D'EXPLOITATION
- Qu'est-ce qu'un système d'exploitation ?
- Connaître les systèmes d'exploitation du marché

LE LAN
- Présentation des LAN
- Les topologies
- Les réseaux Ethernet
- Le WIFI

EXTENSION D'UN RÉSEAU LAN
- Savoir ce qu'est : un réseau PAN, MAN, SAN et WAN
- Savoir ce qu'est un routeur et à quoi il sert

LE PROTOCOLE IP
- La suite de protocoles TCP/IP
- L'adressage IP
- Le routage

PROTOCOLES ET APPLICATIONS
- Les protocoles de la couche transport
- Les protocoles de la couche application

LA SÉCURITÉ
- Pourquoi sécuriser un réseau ?
- Les différents types de protection
- Les protocoles

INTRODUCTION À LA VOIX ET AUX TÉLÉPHONES IP
- Présentation et historique
- Architectures VoiP et ToiP
- QoS

L'ADMINISTRATION DE RÉSEAUX
- Pourquoi administrer son réseau?
- Quelle méthode appliquer ?
- L'architecture utilisée

INTRODUCTION AUX TECHNOLOGIES LES PLUS RÉPANDUES DANS LES RÉSEAUX D'ENTREPRISES
- La virtualisation avec VMWare
- Le client léger de Citrix
- Les bases de données avec MS SQL Server
- La gestion de parc avec SCCM 2007
- Les outils du Web
- La messagerie avec Exchange/ Outlook
- La communication unifiée

RES 212

COMMENT EXPLOITER UN RÉSEAU ?

OBJECTIFS

Cette formation présente comment les tâches du réseau de l'entreprise sont exploitées. Cette formation qui est sur mesure s'adapte et dépend donc du réseau du client.

PUBLIC

Administrateur

1 JOUR

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION
- Objectifs de la formation
- Approche et méthodologie

GÉNÉRALITÉS
- Mise à jour d'un IOS
- Gestion des comptes d'accès

RÉSEAU
- Gestion des interfaces
- Gestion des VLAN
- Gestion du STP
- Gestion du VTP
- Gestion du NAT
- Gestion des routes

SÉCURITÉ
- Gestion des ACL
- Gestion des comptes VPN nomades
- Gestion des VPN site à site
- Gestion des interfaces 802.1x

Frame IP Formation

RES 213

ADMINISTRER AVEC CISCO ACS 5.0

OBJECTIFS

Cette formation vous permettra d'acquérir toutes les connaissances nécessaires à la sécurité des réseaux dans le monde du SI.

PUBLIC

Responsable sécurité / réseau. Ingénieur système et réseau

PRÉREQUIS

Bonnes connaissances en administration réseau avec équipements Cisco et en sécurité informatique

3 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

LES PROTOCOLES RADIUS ET TACACS+

L'INSTALLATION D'ACS 5.0

DIFFÉRENCES ENTRE ACS 4.2 ET 5.0

LES LICENCES ACS

LES SCÉNARIOS D'UTILISATION D'ACS

L'ADMINISTRATION D'ACS

- Interface
- Gestion des utilisateurs
- Configuration de base
- Les ressources réseau
- Les groupes
- Les équipements réseau et les clients AAA

LES UTILISATEURS ET LES « IDENTITY STORES »

- Les attributs (standard, utilisateur…)
- Magasin d'identité
- Interne
- LDAP
- AD
- Les certificats

LES POLICES DE CONTRÔLE D'ACCÈS

- Les conditions
- Les autorisations et permissions
- La création de polices d'accès

LE MONITORING ET REPORTING

- Le dashboard
- Les alarmes

Tallen SI Formation

RES 214

ADMINISTRATION CISCOWORKS LMS 4.0

OBJECTIFS

Cette formation traite des fondamentaux de l'administration réseau, de l'installation, du paramétrage et de l'utilisation des différents modules de CiscoWorks. Elle vous permettra d'acquérir les connaissances nécessaires à la mise en oeuvre de la supervision réseau avec CiscoWorks dans un environnement Cisco.

PRÉREQUIS

Bonnes connaissances en administration réseau avec équipements Cisco. Expérience requise dans l'installation et la configuration de routeurs Cisco.

4 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION À CISCOWORKS

- Les bases de l'administration réseau
- Présentation de la gamme CiscoWorks
- Installation et déploiement de CiscoWorks
- Intégration de CiscoWorks avec d'autres plates-formes de supervision : HPOV & XML

PRISE EN MAIN DE CISCOWORKS

- L'accès au serveur
- Navigation et ergonomie
- La gestion des utilisateurs
- Configuration des bases de données DCR, Campus, RME
- DFM et IPM
- CiscoView : présentation et utilisation

RME

- Gestion de l'inventaire
- Gestion des modifications
- Créations de vues
- Gestion des contrats

CAMPUS MANAGER

- Les services de topologie
- Utilisation de User Tracking
- Utilisation de Path Analysis
- Gestion des modifications
- Créations de vues
- Gestion des contrats

GESTION DES CONFIGURATIONS

- Paramétrage de CiscoView
- Utilisation des outils de RME : Configuration archive, configuration Editor, NetConfiguration, Network Show commandes, software Image Manager et change Audit Services
- Gestion des VLAN
- Gestion des images IOS

RES 215

ÉTAT DE L'ART CISCOWORKS LMS 3.2

OBJECTIFS

Cette formation traite des fondamentaux de l'administration réseau, de l'installation, du paramétrage et de l'utilisation des différents modules de CiscoWorks. Elle vous permettra d'acquérir les connaissances nécessaires à la mise en oeuvre de la supervision réseau avec CiscoWorks dans un environnement Cisco.

PRÉREQUIS

Bonnes connaissances en administration réseau avec équipements Cisco. Expérience requise dans l'installation et la configuration de routeurs Cisco

4 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION À CISCOWORKS 3.2

- Les objectifs de l'administration réseau
- Présentation de LMS 3.2

CISCOWORKS ASSISTANTS (CA)

- Fonctions
- Topologies

COMMON SERVICES (CS)

- Fonctions
- Topologies

CAMPUS MANAGER (CM)

- Fonctions
- Topologies

RESSOURCE MANAGER ESSENTIALS (RME)

- Fonctions

INTERNETWORK PERFORMANCE MONITOR (IPM)

- Fonctions et Topologies

DEVICE FAULT MANAGER (DFM)

- Fonctions
- Architecture
- Terminologies
- Notifications

CISCOVIEW

DEVICE CENTER

HUM

ATELIERS 1 : MISE À JOUR DES IOS

ATELIERS 2 : GESTION DES CONFIGURATIONS

ATELIERS 3 : UTILISATION DE DFM

RES 216

METTRE EN OEUVRE LA QoS LAN CISCO

OBJECTIFS

Cette formation est conçue pour donner aux participants une connaissance parfaite de la QoS IP et Ethernet. Nous détaillerons les modèles Differentiated Services (Diffserv), Integrated Services (IntServ) and Best Effort. Puis nous présenterons et mettrons en place notamment par le biais de Travaux Pratiques les techniques permettant de mettre en place la QoS que sont : la classification, le marquage, la gestion de la congestion, l'évitement de la congestion et la contention de trafic.

PUBLIC

Architectes, administrateurs et ingénieurs réseau.

PRÉREQUIS

Niveau CCNA

4 À 5 JOURS

POINTS CLÉS DU PROGRAMME

INTRODUCTION

- Pourquoi faire de la QoS ?
- Les modèles de QoS (intserv, diffserv, best effort)
- Où placer la QoS ?

LA CLASSIFICATION ET LE MARQUAGE

- Présentation de ces techniques
- Marquage niveau 2 et niveau 3
- Classification avec le Modular QoS CLI (MQC), NBAR et le marquage
- Classification dans les tunnels (VPN)
- TP : mise en oeuvre de techniques de marquage niveau 2 et 3, ainsi que d'une classification liée à ce marquage

GESTION DE LA CONGESTION

- Présentation du queuing
- Mise en file (queuing) FIFO, PQ, CQ
- Les mécanismes WFQ, CB-WFQ, LLQ, WRR…
- TP : mise en oeuvre d'un système de gestion de congestion LLQ

ÉVITEMENT DE LA CONGESTION

- Pourquoi utiliser ces mécanismes ?
- RED
- CB-WRED

LE SHAPPING ET LE POLICING

- Présentation de ces techniques
- CB-shapping /CB-policing
- TP : mise en place de la technique de shapping sur des routeurs Cisco

TROUBLESHOOTING : APPRENDRE À LIRE LA QoS (CHAPITRE COMPLET PRATIQUE : TP)

- Les commandes de visualisation
- Les debug
- Grapher en SNMP ses classes de QoS
- Validation des SLA de son infrastructure avec IP SLA

RES 217

CONFIGURER ET ADMINISTRER DES SWITCH HP

OBJECTIFS

Les commutateurs sont omniprésents dans les réseaux d'entreprise. Dans ce domaine, HP occupe une place très importante parmi les constructeurs. Pour exploiter pleinement cette technologie, les experts doivent savoir déployer et gérer efficacement la commutation HP de niveau 2 ou 3. Vous apprendrez comment ces commutateurs sont configurés et les techniques pour optimiser des réseaux commutés.

PUBLIC

Gestionnaires réseau, techniciens, consultants et ingénieurs impliqués dans la conception, la mise en oeuvre et le dépannage de réseaux avec des commutateurs HP.

PRÉREQUIS

Bonnes connaissances théoriques et pratiques des infrastructures réseau. Connaissances générales sur TCP/IP et le modèle OSI

2 JOURS

POINTS CLÉS DU PROGRAMME

LES FONDEMENTS DU SWITCHING

- Définitions et concepts
- Rôle des switchs
- Switching niveau 2, niveau 3 du modèle OSI
- Les aspects architecturaux : communication, interconnexion des éléments…

GÉNÉRALITÉS D'ADMINISTRATION DES SWITCHS HP

- Généralités sur la configuration et l'administration de switchs
- Mise en oeuvre sur les switchs HP apprentissage des commandes
- L'utilisation des différentes interfaces de configuration
- Configurations de base

CONFIGURATIONS AVANCÉES

VLAN : GÉNÉRALITÉS

- Concepts des réseaux locaux virtuels (VLAN)
- Leur utilisation dans les réseaux
- Comprendre les mécanismes d'encapsulation
- Les normes (802.1Q)
- Configurer et mettre en place des VLAN
- Schéma de priorité IEEE 802.1p
- Routage entre LAN avec la commutation multicouche

DÉPLOIEMENT DE VLAN

- Évaluation des effets du trafic de diffusion
- Limitation de la taille des domaines de broadcast à l'aide de VLAN
- Différences entre les VLAN statiques et dynamiques
- Activation des VLAN par port
- Migration vers des VLAN standard

INTEROPÉRABILITÉ MULTIVENDEUR AVEC LA NORME 802.1Q

802.1X

- Intérêt du 802.1X
- Moyens d'authentification
- Configuration de serveur Radius

SPANNING TREE

- Intégration de la résilience (tolérance aux pannes)
- Gestion de la redondance de liens avec STP, MSTP
- Équilibrage de charges

DEBUG

- Compréhension du problème
- Méthodologie de résolution
- Commandes utiles

RES 218

CONFIGURATION DES SERVICES RÉSEAUX TCP / IP

OBJECTIFS

Développer et administrer un réseau

PUBLIC

Administrateurs système

PRÉREQUIS

Connaissance de base des réseaux informatiques. Connaissance de base des protocoles TCP / IP.

1 JOUR

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

MODÈLES DE COMMUNICATION

- Le modèle OSI
- Le modèle TCP/IP

LES RÉSEAUX TCP/IP

- Adressage
- Masques de sous réseaux
- Ports et sockets
- Résolution d'adresses Ethernet
- Résolution d'adresses IP

CONFIGURATION DE TCP/IP

- Le fichier / etc / sysconfig / network
- Le fichier/ etc / sysconfig / network-scrpts / ifcg-eth0

COMMANDES DE BASE

- ifconfig, hostname, uname, ping, traceroute, netstat

UTILITAIRES TCP/IP

- wget, Telnet, FTP, SHT, SCP, SHT-keygen, rlogin

SERVICES RÉSEAU

- inetd
- TCP Wrapper
- xinetd

OUTILS POUR ÉCOUTER

- TCPdump
- Ethereal

ROUTAGE

- Routage statique
- Routage dynamique

CONFIGURER UN SERVEUR DNS

- Présentation
- Installation
- Configuration

CONFIGURER UN SERVEUR DHCP

- Présentation
- Installation
- Configuration

CONFIGURER UN SERVEUR D'HORLOGE

- Présentation
- Installation
- Configuration

CONFIGURER UN SERVEUR FTP

- Présentation
- Installation
- Configuration de base
- Configuration du serveur FTP anonyme
- Configuration d'une zone d'upload

Tallen Si Formation

RES 219

SUPERVISER SON RÉSEAU AVEC NAGIOS

OBJECTIFS

Cette formation est conçue pour donner aux participants l'opportunité de monter leur machine de supervision et de monitoring de façon autonome. Elle a également pour but de montrer l'importance et la criticité d'avoir ce genre de machine dans le système d'information.

PUBLIC

Administrateurs réseaux et systèmes, ingénieurs réseaux, support informatique.

PRÉREQUIS

De solides connaissances en réseau et système Linux ainsi que sur le protocole SNMP

3 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION ET RAPPELS SUR LE RÉSEAU

- Le modèle OSI
- Le modèle TCP/IP
- Ethernet
- Adressage IP

L'OS LINUX

- Historique
- Les distributions
- La licence GPL
- Caractéristiques du système

INTRODUCTION À LA SUPERVISION ET LE MONITORING

- Intérêts et importance
- Les systèmes de supervision et de monitoring existants
- Introduction à Nagios
- Introduction à Cacti
- Introduction à Nagvis

INSTALLATION DE L'OS

- La marche à suivre / les instructions
- Choix de la distribution
- Dimensionnement de la machine
- Accompagnement à l'installation
- Accompagnement post-install

INSTALLATION DE NAGIOS

- Téléchargement des sources
- Compilation et installation
- Configuration / explication du fonctionnement
- Pour aller plus loin (créer ses propres scripts, introduction à NRPE, ...)
- Intégration de Nagvis

INSTALLATION DE CACTI

- Téléchargement des sources
- Compilation et installation
- Configuration / explication du fonctionnement

SÉCURITÉ

- SE 301 Introduction à la sécurité des réseaux
- SE 302 La sécurité de votre Système d'Information
- SE 303 Concevoir et mettre en œuvre la sécurité du SI
- SE 304 Mettre en œuvre la sécurité des réseaux
- SE 305 Sécuriser votre infrastructure - Les stratégies et outils
- SE 306 Construire un réseau WiFi sécurisé
- SE 307 Politique de sécurité - Les firewalls
- SE 308 Palo Alto
- SE 309 Administration Checkpoint
- SE 310 Sécuriser un réseau avec Checkpoint
- SE 311 Sécuriser un réseau avec Cisco ASA - Les fondamentaux
- SE 312 Sécuriser un réseau avec Cisco ASA - Perfectionnement
- SE 313 Installation et paramétrage des produits Sonicwall
- SE 314 F5 BIG-IP : load Balancing, APM
- SE 315 Le hacking - Comment se protéger du piratage informatique
- SE 316 Détecter une intrusion dans son SI
- SE 317 Réaliser un audit de sécurité informatique
- SE 318 Sécuriser un système Linux

Avec la démocratisation d'Internet et des moyens de communication, la sécurité des réseaux est devenue un enjeu majeur. En effet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs et il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise à Internet.

Parce que les données d'une entreprise sont privées et ne doivent pas tomber à la portée de tous, celles-ci doivent être protégées des agressions extérieures. Parce que l'informatique évolue en permanence, une vigilance constante est de rigueur.

C'est pourquoi nous vous proposons de prendre en charge l'administration et la maintenance au quotidien

Sécuriser son réseau avec FrameIP et TallenSI, c'est garantir à son entreprise une sécurisation optimale des données.

SE 301

INTRODUCTION À LA SÉCURITÉ DES RÉSEAUX

OBJECTIFS

Évaluer la nature des risques introduits par les réseaux IP dans les SI. Vous approprier la terminologie et les concepts de la sécurité des réseaux IP. Mettre en oeuvre des équipements de sécurité.

PUBLIC

Décideur, architecte, administrateur réseau et système concernés par les problèmes de sécurité, responsable de l'audit informatique, chef de projet informatique.

3 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

CONCEPTS FONDAMENTAUX DE LA SÉCURITÉ

Protection de l'information
Domaines de sécurité (physique, logique, réseau, système)

TRANSACTIONS

Problèmes de sécurité liés à IP (réseaux et applications)
Menaces, risques, vulnérabilités

TYPES D'ATTAQUES

Attaques passives
Attaques actives
Parades aux attaques

SERVICES DE SÉCURITÉ

Critères DICP
Analyse de risques

TECHNOLOGIES DE FILTRAGE

Principes
Niveaux de filtrage : réseaux, applications, données
Firewall/Proxy/Anti-virus : principes, fonctions

TECHNOLOGIES DE SCELLEMENT

Intégrité des données
Algorithme de hachage (MD5, SHA-1)

TECHNOLOGIES DE CHIFFREMENT

Chiffrement symétrique
Chiffrement asymétrique
Infrastructure des clés publiques (PKI)

ARCHITECTURES DE SÉCURITÉ

VLAN
Mode : bastion, DMZ, DMZ étendue
VPN
Étude de cas Internet/ Intranet/ Extranet : architectures, règles de sécurité

IPSEC

Fonctions de sécurité
Architecture
Modes : transport, tunnel
Protocoles : AH, ESP,
Gestion des clés : IKE

PROTOCOLES DE SÉCURITÉ SUR INTERNET / INTRANET

S-HTTP, S-MIME, SSL, PCT, TLS, PGP, RADIUS

DIMENSION ORGANISATIONNELLE ET JURIDIQUE DE LA SÉCURITÉ

Conduire une politique de sécurité réseau
Aspects juridiques
Projet sécurité

TRAVAUX PRATIQUES

Règles de sécurité Firewall et Proxy
Déclenchement d'une attaque et parade associée
Translation d'adresses
Filtrage d'adresses réseau via une ACL, filtrage applicatif via un proxy

SE 302

LA SÉCURITÉ DE VOTRE SYSTÈME D'INFORMATION

OBJECTIFS

La réussite d'un projet informatique dépend d'un nombre de facteurs important, certains sous notre contrôle et d'autres non. L'objectif de cette formation est de vous apporter les bonnes pratiques autant d'un point de vue organisationnel et technique que relationnel afin de pouvoir anticiper et réagir rapidement, et ainsi conserver la maîtrise de votre projet.

PUBLIC

Toute personne chargée du pilotage d'un projet informatique.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION

Présentation des risques pour une entreprise
Historique du hack et dates clés
Quelques exemples de cybercriminalité

MÉTHODES D'INTRUSION

Attaques par le stack IP
Les attaques applicatives (DNS, HTTP, SMTP…)
Les injections de code
Le «social engineering»
Sécurisation des locaux

PRINCIPALES MENACES : LES POSTES UTILISATEURS

Virus, chevaux de Troie, spyware…
Sécurité du poste client (Firewall local, anti-virus, anti-spyware…)
Le danger des périphériques amovibles
La sécurité intégrée : Windows vs Linux

LES RÉSEAUX SANS FIL

Attaques spécifiques (Wardriving, sécurité Wep et EAP)
Sécurisation des bornes (SSID, fi ltrage MAC)
Authentification utilisateur (EAP, certificat, token…)
Le Bluetooth

PROTÉGER SON RÉSEAU DE L'ENVIRONNEMENT EXTÉRIEUR

Proxy et reverse proxy
Principe des fi rewalls, périmètre fonctionnel
Les DMZ
Évolution de l'offre firewall (appliance, VPN, IPS, UTM…)

LA SÉCURITÉ VPN

Le concept VPN
La technologie IPSec
SSL vs IPSEC
Les VPN avec différents OS
Les offres VPN Opérateurs (VPN IPSEC et VPN MPLS)

GESTION ET SUPERVISION DU SI

Les normes en vigueurs
Définition de tableaux de bord
Le rôle du RSSI
Les audits de sécurité
Les scanners de vulnérabilité et tests d'intrusion
Veille technologique et mise à niveau
Notion de PRI / PRA : savoir réagir en cas d'incident
Travaux pratiques
Présentation des outils : Nessus…
Intrusion dans un service du SI

SE 303

CONCEVOIR ET METTRE EN OEUVRE LA SÉCURITÉ DU SI

OBJECTIFS

Il est devenu primordial de savoir faire face aux attaques virales et autres actes de piratage pour protéger les données de l'entreprise et garantir l'intégrité et le bon fonctionnement de son système d'information. Les participants découvriront les principaux concepts liés à la sécurité des réseaux ainsi que les stratégies et les outils permettant de protéger les infrastructures d'entreprise.

PUBLIC

Responsables informatiques, administrateurs réseaux, techniciens, Webmaster, responsables de la sécurité informatique.

PRÉREQUIS

Avoir une bonne connaissance des réseaux Windows ou Unix ou du protocole TCP /IP

4 JOURS

POINTS CLÉS DU PROGRAMME

DÉVELOPPER LA POLITIQUE DE SÉCURITÉ

La sécurité et la continuité
Les applications et les outils disponibles

LA SÉCURITÉ DES SYSTÈMES UNIX ET WINDOWS

La gestion de l'authentification
La gestion de services réseau

LA SÉCURITÉ CLIENT

Les certificats clients
Les options de sécurité des navigateurs

LA SÉCURITÉ SERVEUR

L'authentification des utilisateurs
Protéger l'accès au serveur

MISE EN PLACE DE L'INTRANET VIA LE RÉSEAU PUBLIC

Le déploiement d'un réseau privé virtuel
Les méthodes d'authentification

LES MÉTHODES DE PIRATAGE ET LES TYPES D'ATTAQUES

Les attaques sur les protocoles
Les faiblesses des services
Les virus et chevaux de Troie

LA MISE EN PLACE DE CERTIFICATS

Les serveurs de certificats
Les certificats numériques

LES TECHNIQUES CRYPTOGRAPHIQUES

L'objectif du chiffrement
Les normes et leurs possibilités

LES SERVEURS PROXY

L'architecture d'un proxy
La gestion des proxies avec des firewalls

ARCHITECTURE ET CONFIGURATION DES FIREWALLS

Les différents types de firewalls
Les règles du filtrage
Les règles de la translation d'adresse
La mise en oeuvre d'une DMZ
L'intégration d'un firewall dans le réseau d'entreprise

DÉTECTION ET SURVEILLANCE DES FAIBLESSES

Les informations à surveiller
Analyse du trafic réseau

MISE EN PLACE DE LA SÉCURITÉ DES DONNÉES DE L'ENTREPRISE

Évaluation des besoins de l'entreprise
Règles de la mise en place d'un plan de sécurité
La veille technologique

SE 304

METTRE EN OEUVRE LA SÉCURITÉ DES RÉSEAUX

OBJECTIFS

Savoir concevoir et réaliser une architecture de sécurité adaptée. Mettre en oeuvre les principaux moyens de sécurisation des réseaux. Disposer d'une première approche sur la sécurisation des serveurs. Découvrir les obligations légales inhérentes à la sécurité

PUBLIC

Toute personne en charge de la sécurité d'un système d'information ou intervenant sur le réseau ou la mise en place de serveurs d'entreprises

PRÉREQUIS

Utilisation courante de Windows et des équipements constitutifs d'un réseau, connaissances des réseaux et TCP/IP.

4 JOURS

POINTS CLÉS DU PROGRAMME

L'ENVIRONNEMENT

Le périmètre (réseaux, systèmes d'exploitation, applications)
Les acteurs (hacker, responsable sécurité, auditeur, vendeur et éditeur, sites de sécurité)
Les risques
La protection
La prévention
La détection

LES ATTAQUES

Les intrusions de niveau 2
Les intrusions de niveau 3 (IP)
Les attaques logiques
Les attaques applicatives

LES PROTECTIONS

Au niveau des commutateurs d'accès
Au niveau sans-fil
Au niveau IP
Protection des attaques logiques
Protection des attaques applicatives

LA SÉCURISATION DES ACCÈS DISTANTS

Établissement d'un VPN
Choix cryptographique
VPN IPSec : serveur ou boîtier spécialisé ou UTM ?
Client logiciel ou matériel ?
VPN SSL : serveur
Appliance spécialisée ou UTM ?
Principe du NAC

MONITORING ET PRÉVENTION

Sondes IDS
SysLog Serveur
Exploitations des logs
IPS : boîtiers dédiés, fonctionnalités du routeur

EXEMPLES D'ARCHITECTURES

Exemple d'une entreprise monosite
Connexion des nomades
Exemple d'entreprises multisites

CADRE LÉGISLATIF

Rappel sur le cadre légal
Rappel sur l'application de la LSF

SE 305

SÉCURISER VOTRE INFRASTRUCTURE - STRATÉGIES ET OUTILS

OBJECTIFS

Cette formation a pour objectif de donner une vision technique et transverse de la sécurité des infrastructures réseaux informatiques. Durant cette formation, des principes généraux (méthodologie, démarche et organisation) sont présentés ainsi qu'un état de l'Art des technologies avec les composants des architectures de sécurité.

PUBLIC

Responsables opérationnels tels que le responsable de la sécurité des systèmes d'information, l'ingénieur sécurité, l'administrateur réseau, le responsable d'exploitation et le chef de projets techniques.

PRÉREQUIS

Avoir des connaissances de base sur les technologies et standards du réseau : Ethernet, adressage Ethernet et IP, TCP/IP, principe du routage, principe de nommage DNS, infrastructure Clients/Serveur ou N-tiers.

5 JOURS

POINTS CLÉS DU PROGRAMME

PROBLÉMATIQUE DE LA SÉCURITÉ INFORMATIQUE ET RÉSEAU

- Analyse du contexte et les chiffres clés actuels
- Ouverture des réseaux et évolution constante des infrastructures
- Fondamentaux de la sécurité informatique et réseau

CONTRE QUI ET QUOI SE PROTÉGER ?

- Taxinomie des attaquants
- Compétences & sophistication des attaques
- Typologies & cinématique des attaques
- Méthodologie de l'attaquant
- Présentation des quelques attaques (ARP poisoning, SQL injection,
- Cross scripting, buffer overflow,
- SSL man in the middle, déni de service, scanner, password cracker)
- Démonstrations
- Que voulons-nous protéger ?

COMMENT SÉLECTIONNER DES PRODUITS DE SÉCURITÉ ?

- Historique
- Les référentiels
- CC
- Critères d'évaluation de sécurité et niveaux de certification
- Processus d'évaluation des produits
- Exemples de quelques produits

PROTECTION ET CLOISONNEMENT DES RÉSEAUX OBJECTIFS - PROTECTION PHYSIQUE ET LOGIQUE

- VLAN, Routeur filtrant? firewalls embarqués (appliance) Réseau et applicatifs
- Proxies et reverse proxies : filtrage de contenu, antivirus,
- Contrôle et enregistrement des flux
- Produits du marché

PROTECTION DES APPLICATIONS, DONNÉES ET CRYPTOLOGIE

- Notions de cryptologie : origine, problématique et terminologie
  Concepts de base,
- principes du chiffrement symétrique et asymétrique, certificats électroniques X509 V3 (clé publique, clé privée)
- Sécurisation des données et PKI (Public Key Infrastructure) : autorité de certification (architecture PKI, entités et rôles), Certificat électronique et cycle de vie du certificat, standards PKCS, déploiement d'une PKI Outils de chiffrement de données

PROTECTION DES COMMUNICATIONS RÉSEAU

- VPN chiffré et technique de tunneling
- Standards SSL V3 et Standard
- IPSec
- SSL Versus IPSec
- Produits du marché

AUTHENTIFICATION DES UTILISATEURS ET ACCÈS AUX APPLICATIONS

- Modes d'authentification
- Technologies d'authentification (carte à puce, USB, Token) Authentification personnelle et Authentification réseau
- Authentification non rejouable OTP (One Time Password) Authentification unique SSO (Single Sign On) : SSO Host et SSO Web

AUDITS DE SÉCURITÉ – OUTILS - SUPERVISION SÉCURITÉ - GESTION DES INCIDENTS

- Méthodologie des audits techniques de sécurité
- Outils d'audit de vulnérabilités réseau, système et applicatif
- Détection d'intrusions réseau : réaction aux incidents et aux sinistres Protocoles sécurisés d'administration des équipements (HTTPS, SSH, SFTP) - Reporting et centralisation des logs des équipements de sécurité
- Patch management

SE 306

CONSTRUIRE UN RÉSEAU WIFI SÉCURISÉ

OBJECTIFS

- Comprendre le fonctionnement des différents protocoles de sécurité
- Savoir choisir les technologies réseau sans fil
- Être en mesure d'identifier les forces et faiblesses de diverses solutions du marché
- Disposer des bonnes pratiques pour la mise en oeuvre d'une solution WiFi sécurisée

PUBLIC

- Administrateurs réseau
- Responsables sécurité en charge d'une architecture possédant des points d'accès sans-fil ou des PC équipés de cartes sans-fil

PRÉREQUIS

Avoir des connaissances sur le WiFi et être autonome avec TCP / IP

2 JOURS

POINTS CLÉS DU PROGRAMME

INTRODUCTION

Rappels sur les réseaux sans fil
Le SSID
Les VLANs

SÉCURISER L'ADMINISTRATION DES ÉQUIPEMENTS RÉSEAUX SANS FIL

Administration par SNMP : le protocole SNMP, SNMP V1 et V2, SNMP V3
Administration par page Web : HTTP, HTTPS
Administration en mode caractère : Telnet, SSH

SÉCURISER LES ACCÈS CLIENTS

Introduction : authentification, association, problématique de la sécurité des réseaux sans fil
Méthodes par défaut : SSID, authentification ouverte, authentification partagée, clé WEP
Outils de hacking et faiblesse de la clé WEP : Airsnort, John the ripper...
Technique de hacking : attaques passive et active, attaque weak IV, attaque par dictionnaire, attaque type bit flip, attaque type IV replay
Méthodes 802.1X : EAP Fast, PEAP, EAP TLS, quelles méthodes 802.1X choisir ?
Standards de sécurité pour les réseaux sans-fil : VPN IPSEC, 802.11i, WPA, WPA 2, TKIP et MIC, Encryption AES
Gestion de la sécurité d'un réseau sans-fil d'entreprise : problématique du vol d'équipement ou du départ d'un employé, la gestion centralisée de la sécurité, intégration dans un domaine active directory, utilisation des comptes utilisateurs Windows, utilisation de one time password (OTP), le serveur AAA
Gestion de la sécurité des bornes type Box : Live box, Free box
Conseils de configuration

SÉCURITÉ SUPPLÉMENTAIRE PAR ADMINISTRATION CENTRALISÉE

L'administration sans fil centralisée avec bornes légères
L'administration centralisée avec bornes intelligentes
Détection des bornes ennemies
Détection d'une tentative de pénétration
Centralisation des politiques de sécurité

SE 307

POLITIQUE DE SÉCURITÉ - LES FIREWALLS

OBJECTIFS

- Appréhender les menaces et les attaques internes et externes du monde IP, les vulnérabilités
- Déterminer les points clefs d'une politique de sécurité
- Comprendre les bons choix pour une architecture sécurisée, tout en conservant un bon niveau de performance
- Décrire les principales vulnérabilités
- Décrire les fonctions d'un firewall
- Classifier les différentes catégories de firewalls
- Déployer et administrer des firewalls

PUBLIC

Techniciens, administrateur réseau, responsable de systèmes d'information

PRÉREQUIS

Avoir des bases en réseau

3 JOURS

POINTS CLÉS DU PROGRAMME

INTRODUCTION

Concepts de sécurité : les points clefs
La sécurité dans les réseaux IP

RAPPELS SUR TCP/IP ET LES SERVICES INTERNET

Points clefs de l'adressage IP
Le routage
Les services TCP/IP : les ports et les sockets
Mécanismes d'une session TCP/IP

VULNÉRABILITÉS ET ATTAQUES

IP, TCP
Services (SMTP, DNS, SNMP, NFS, HTTP, FTP, etc.)

FONCTIONS ET LIMITES D'UN FIREWALL

Concepts et définitions, protection d'un réseau par un firewall
Le filtrage et ses limites, NAT, PAT, ports

FIREWALL ET PERFORMANCES DES RÉSEAUX

La répartition de charges
La haute disponibilité

LES CATÉGORIES DE FIREWALLS

Routeurs filtrants
Firewalls à états
Proxies et firewalls

ARCHITECTURE DE SÉCURITÉ

Les zones démilitarisées
Architectures classiques et ses différentes variantes
Déploiement

ADMINISTRATION DES FIREWALLS

Architecture d'un firewall, règles de sécurité
Le traitement des logs
Supervision et sécurité d'un firewall

LES OFFRES DU MARCHÉ ET DU DOMAINE PUBLIC

Exemples concrets
Conseils pratiques et sources d'information

SE 308

PALO ALTO

OBJECTIFS

Les participants auront acquis des connaissances approfondies sur l'installation, la configuration et la gestion de leurs firewalls. Ils connaîtront aussi les étapes de configuration pour la sécurité, le réseau, la prévention des menaces, les loggings et les fonctionnalités de reporting du système d'exploitation de Palo Alto Networks.

PUBLIC

Administrateurs réseau et sécurité

PRÉREQUIS

Connaître les concepts réseaux (routage switching, adressage IP), connaître les bases de sécurité firewalls

1 JOUR

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

GESTION ET ADMINISTRATION
- GUI, CLI et API
- Administration basic
- PAN-OS et Mises à jours

CONFIGURATION DES INTERFACES
- Niveau 2, Niveau 3, Virtual Wire et mode miroring
- Sous-interfaces
- Security Zones

INTERFACE NIVEAU 3
- Configuration
- Profile de management
- Routage services internes
- DHCP
- Routeur Virtuel
- NAT (Source et destination)
- IV6

APP-ID
- Analyse
- Utilisation des applications dans les règles de sécurités
- Gestion des règles de sécurités

CONTENT-ID
- Antivirus
- Anti-Spyware
- Vulnérabilités
- Filtrage d'URL
- Blocage fichier : WILDFIRE
- Protection des zones de sécurités

DÉCHIFFREMENT
- Déchiffrement SSL entrant et sortant

USER-ID
- Agent d'authentification
- 2 numération des utilisateurs
- Association Utilisateur / adresse ID
- Utilisation des noms dans les règles de sécurités

VPN
- IPSec
- Introduction à Global Protect

HAUTE DISPONIBILITÉ
- Configuration Actif /Passif

PANORAMA
- Groupe de boitiers et modèles
- Règles partagées
- Gestion des configurations
- Collection des logs et gestion des rapports

SE 309

ADMINISTRATION CHECKPOINT

OBJECTIFS

Cette formation vous fera découvrir les nouveautés apportées par la dernière mouture des produits Check Point, la version R70. À l'issue, vous serez capable de mettre en place et gérer une politique de sécurité, la translation d'adresses (NAT), ou encore le module Intrusion Prevention System (IPS).

PUBLIC

Technicien, administrateur et ingénieur système / réseau / sécurité.

4 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION
- La gamme checkpoint 2012 (pare feu, appliances dédiées)
- Les software blades
- Secure platform et Gaia

INSTALLATION
- Les modes de déploiement
- Configuration

POLITIQUE DE SÉCURITÉ
- Gestion des règles de filtrage simple
- Identity Awarness
- Application Control

TRANSLATION D'ADRESSE (NAT)
- Translation automatique
- Translation manuelle

VPN
- VPN site a site
- VPN remote access
- VPN SSL

ADMINISTRATION
- Supervision
- Smart tracker et Smart view Monitor
- Sauvegarde / Restauration de la configuration

SE 310

SÉCURISER UN RÉSEAU AVEC CHECKPOINT

OBJECTIFS

Cette formation vous fera découvrir les nouveautés apportées par la dernière mouture des produits Check Point, la version R70. À l'issue, vous serez capable de mettre en place et gérer une politique de sécurité, la translation d'adresses (NAT), ou encore le module Intrusion Prevention System (IPS).

PUBLIC

Technicien, administrateur et ingénieur système / réseau / sécurité.

4 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION

Les produits Check Point. Nouveautés de la version R70
Les composants

FONCTIONNEMENT ET INSTALLATION

L'architecture en mode distribué et en mode standalone
Le serveur de management. Le protocole SIC
L'interface en ligne de commandes (CLI)
Les commandes de sauvegarde et de restauration
Travaux pratiques

MISE EN PLACE D'UNE POLITIQUE DE SÉCURITÉ

Prise en main de SmartConsole
Démarrer et utiliser SmartDashboard
Gestion des administrateurs et des profils
Politique de sécurité
Gestion des règles
Travaux pratiques

LA TRANSLATION D'ADRESSES (NAT)

Les règles de translation d'adresses
Le NAT «static» et le NAT «hide»
Gestion de l'ARP

LE MONITORING ET LA GESTION DES LOGS

La politique de gestion des logs
Trouver et suivre les connexions avec SmartView Tracker
Le SmartView Monitor, fonctionnalités et seuils d'alerte
Travaux pratiques

AUTHENTIFICATION CLIENT

Les différents types d'authentification : USER, SESSION et CLIENT
SmartDirectory et l'intégration avec LDAP
Travaux pratiques
Mise en place de l'authentification client

LE VPN SITE / SITE

L'architecture
Les bases du chiffrement
Introduction à IKE et IPSec
L'autorité de certification (CA)
Le Domain-Based VPN
Travaux pratiques
Mise en place d'un tunnel IPSec site à site

LE VPN CLIENT / SITE

L'accès distant VPN IPSec
Introduction au VPN SSL
Le SecuRemote / SecureClient
La Desktop Policy
Travaux pratiques

LE FILTRAGE DE CONTENU

La protection antivirus
Le filtrage WEB
Les e-mails et l'anti-spam
Travaux pratiques

LE MODULE IPS

Présentation d'IPS
Les vulnérabilités et failles de sécurité
Le Web Intelligence, Application Intelligence et Network Security
Les profils de sécurité IPS et IDS
Travaux pratiques
Exemple de protection contre les vulnérabilités avec le module IPS

SE 311

SÉCURISER UN RÉSEAU AVEC CISCO ASA - FONDAMENTAUX

OBJECTIFS

- Être en mesure d'expliquer les fonctions des trois types de firewalls utilisés pour sécuriser les équipements réseaux
- Appréhender les technologies et les caractéristiques des solutions de sécurité Cisco
- Savoir comment configurer un Firewall
- Apprendre à utiliser la solution graphique d'administration des ASA
- Maîtriser la configuration et la maintenance des VPN

PUBLIC

- Responsables de l'implémentation et de la maintenance des ASA
- Responsables sécurité

PRÉREQUIS

- Avoir un niveau équivalent au CCNA
- Posséder des bases sur les environnements Microsoft Windows
- Être familiarisé avec les notions et concepts de sécurité réseau

5 JOURS

POINTS CLÉS DU PROGRAMME

INTRODUCTION DES TECHNOLOGIES ET CARACTÉRISTIQUES DES FIREWALLS

Les Firewalls
Les solutions de sécurité

FAMILLE DES FIREWALLS CISCO PIX ET ASA

Les modèles et caractéristiques des solutions de sécurité Cisco
Les licences des solutions de sécurité Cisco

DÉMARRER AVEC LES SOLUTIONS DE SÉCURITÉ CISCO

Interface utilisateur
Gestion de fichiers
Les niveaux de sécurité des solutions Cisco
Configuration requise et ASDM Cisco
Préparation à l'utilisation d'ASDM Cisco
Navigation dans ASDM Cisco

CONFIGURATION D'UNE SOLUTION DE SÉCURITÉ

Configuration basique
Contrôle de l'état d'une solution de sécurité
Réglage du temps et support de NTP
Paramétrage de syslog

CONFIGURATION DES TRANSLATIONS ET CONNEXIONS

Les protocoles de transport
Compréhension du NAT
Compréhension du PAT
Translations statiques
Cookies TCP SYN et contrôles des connexions

LISTE DE CONTRÔLES D'ACCÈS (ACLS) ET FILTRAGE DE CONTENU

Configuration des ACL
Filtrage des codes malicieux
Filtrage des URL
Traceur de paquets

CONFIGURATION DES GROUPES D'OBJET

L'essentiel
Configuration

ROUTAGE ET COMMUTATION SUR DES SOLUTIONS DE SÉCURITÉ CISCO

Capacités des VLAN
Routage statique
Routage dynamique

CONFIGURATION AAA (AUTHENTIFICATION, AUTORISATION AND ACCOUNTING)

Introduction AAA
Configuration d'une base de données utilisateur
Installation du Cisco Secure ACS sur une plateforme Windows 2000
Configuration d'une authentification Cut-Through Proxy
Invites d'authentification et déconnexions
Configuration des autorisations
Configuration de la traçabilité

CONFIGURATION DE LA POLITIQUE MODULAIRE

Vue d'ensemble des politiques modulaires
Vue d'ensemble des Class Map
Vue d'ensemble des Policy Map
Configuration des politiques modulaires avec Cisco ASDM
Configuration d'une politique pour la gestion du trafic
Affichage des composants de politiques modulaires

CONFIGURATION DE LA PRISE EN CHARGE DE PROTOCOLES AVANCÉS

Prise en charge de protocoles avancés
Application du protocole d'inspection
Support multimédia

CONFIGURATION DE LA DÉTECTION DE MENACES

Vue d'ensemble
Détection basique de menaces
Balayage d'une détection de menaces
Configuration et analyse des statistiques d'une détection de menaces

CONFIGURATION D'UN VPN SITE À SITE AVEC UNE CLÉ PARTAGÉE

Sécuriser les VPN
Fonctionnement d'IPsec
Préparation à la configuration VPN IPsec
Configuration d'un VPN site à site avec une clé partagée
Test et Vérification de la configuration du VPN

CONFIGURATION D'UN VPN ACCÈS DISTANT

Introduction à Cisco Easy VPN
Vue d'ensemble de Cisco VPN Client
Configuration d'accès distant VPN
Configuration des utilisateurs et des groupes

CONFIGURATION ASA POUR UN VPN SSL

Vue d'ensemble VPN SSL
Utilisation du Wizard VPN SSL pour configurer du VPN SSL sans client
Vérification de la configuration VPN SSL

CONFIGURATION DU FIREWALL EN MODE TRANSPARENT

Vue d'ensemble
Franchissement d'une solution de sécurité en mode transparent
Configuration du firewall
Surveillance et suivie du firewall en mode transparent

CONFIGURATION DES CONTEXTES DE SÉCURITÉ

Vue d'ensemble des contextes de sécurité
Activation du mode de contexte multiple
Paramétrage d'un contexte de sécurité
Allocation de ressources pour les contextes de sécurité
Gestion des contextes de sécurité

CONFIGURATION DE LA FONCTION FAILOVER

Comprendre le principe du failover
Configuration d'interfaces redondantes
Configuration du LAN-Based Failover
Configuration du Failover
Exécution de commandes à distance

GESTION DE LA SOLUTION DE SÉCURITÉ

Gestion de l'accès au système
Configuration des commandes d'autorisation
Gestion des configurations
Gestion des images et des clés d'activations

Frame IP Formation

SE 312

SÉCURISER UN RÉSEAU AVEC CISCO ASA - PERFECTIONNEMENT

OBJECTIFS

- Être capable de configurer les politiques de NAT en fonction du trafic ainsi que les VLAN
- Maîtriser la configuration d'un protocole de routage
- Comprendre les composants et les fonctionnalités d'IPSec et comprendre comment les certificats digitaux sont utilisés
- Être en mesure de configurer la solution de sécurité ASA 5505 comme VPN client hardware
- Acquérir les compétences permettant l'identification des fonctionnalités du client SSL

PUBLIC

Responsable sécurité, ingénieur, administrateur systèmes et réseaux

PRÉREQUIS

- Avoir suivi la formation «Sécuriser un réseau avec ASA - les fondamentaux » ou connaissances équivalentes
- Être certifié CCNA
- Posséder des bases sur les environnements Microsoft Windows

5 JOURS

POINTS CLÉS DU PROGRAMME

CONFIGURATION ET VÉRIFICATION DU NAT, DU ROUTAGE DYNAMIQUE, ET DU SWITCHING SUR LES SOLUTIONS DE SÉCURITÉ

Configurer les VLAN en utilisant ASDM
Configurer les protocoles de routage dynamique et les redistributions de route en utilisant ASDM
Configurer les politiques de NAT en utilisant ASDM

CONFIGURATION ET VÉRIFICATION DE L'INSPECTION DES PROTOCOLES APPLICATIFS ET LA POLITIQUE MODULAIRE POUR LES SOLUTIONS DE SÉCURITÉ

Décrire les capacités de traitement des protocoles applicatifs sur la solution de sécurité
Configurer et vérifier l'inspection des protocoles applicatifs en utilisant ASDM
Configurer et vérifier la politique modulaire en utilisant ASDM

CONFIGURER UNE CONNEXION SÉCURISÉE EN UTILISANT DES VPN IPSEC

Décrire les points clés et les capacités des certificats digitaux
Décrire comment utiliser l'inscription des certificats digitaux avec la solution de sécurité et le client VPN Cisco
Configurer les VPN accès distants avec des certificats digitaux en utilisant ASDM
Configurer les clients VPN IPsec avec des certificats digitaux en utilisant ASDM
Configurer un VPN site à site avec des certificats digitaux en utilisant ASDM
Configurer un VPN accès distant avancé en utilisant ASDM
Configurer un ASA 5505 comme client de l'accès distant en utilisant ASDM
Configurer de la QoS pour le trafic passant dans un tunnel en utilisant ASDM

CONFIGURER ET VALIDER UNE CONNEXION SÉCURISÉE EN UTILISANT DU VPN SSL

Décrire les fonctionnalités et les capacités d'un VPN SSL
Configurer et vérifier l'autorité de certification locale en utilisant ASDM
Configurer et vérifier des smart tunnels des plug-ins et des liens en utilisant ASDM
Configurer et vérifier la redirection de port en utilisant ASDM
Configurer la solution de sécurité pour l'accès client VPN SSL
Configurer le client AnyConnect
Configurer le Cisco Secure Desktop en utilisant ASDM
Configurer le Dynamic Access Policies en utilisant ASDM

CONFIGURER ET VALIDER LES MODULES SSM

Expliquer la fonction d'un module AIP-SSM et CSC-SSM dans un réseau
Configurer et valider le module AIP-SSM
Configurer et valider le module CSC-SSM

Tallen Si Formation

SE 313

INSTALLATION ET PARAMÉTRAGE PRODUITS SONICWALL

OBJECTIFS

Acquérir une grande expertise dans l'installation et la maîtrise des produits SonicWALL

PUBLIC

Techniciens, Consultants en technologie de réseaux, Chef de projet technique.

PRÉREQUIS

Concepts réseaux de base, topologies réseaux, modèle OSI, TCP/IP, adressages réseaux, masque de sous réseaux, translation d'adresses, concept de base sur les routeurs, connaissances du protocole IPSec.

2 JOURS

POINTS CLÉS DU PROGRAMME

FUNCTIONAL SOLUTION 1 : INFRASTRUCTURE

Initial Setup & Configuration
Firewall setup and registration
Network Address Translation (NTA)
Inbound server access configurations

FUNCTIONAL SOLUTION 2 : SCALABILITY & RELIABILITY

WAN ISP failover and outbound load balancing
Policy Based Routing

FUNCTIONAL SOLUTION 3 : SERVER ACCESS AND CONTENT CONTROL

Virtual Private Networking (VPN)
GVC w/Local Database
GVC w/LDAP Authentication
CFS w/LDAP Authentication
CFS w/LDAP Authentication using SSO

FUNCTIONAL SOLUTION 4 : UNIFIED THREAT MANAGEMENT (UTM)

UTM

SE 314

F5 BIG-IP : LOAD BALANCING, APM

OBJECTIFS

Cette formation à pour objectif la compréhension des notions essentielles de load balancing.
La configuration des F5 BIG IP en tant de load balancer

PUBLIC

Architectes, administrateurs, consultants et ingénieurs réseaux

PRÉREQUIS

De solides connaissances en réseau. Notions en load balancing. Notions en fonctionnement / configuration des serveurs Web

3 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION ET RAPPEL

Le modèle OSI
Fonctionnement des serveurs Web

PRÉSENTATION

Le partage de charge
Les problématiques associées
La gamme F5 BIG IP
Mode de fonctionnement

ADMINISTRATION

Installation / configuration
Prise en main
Configuration réseau
Log
TP : Installation, configuration de base

LOAD BALANCING

Généralités
Présentation des différents modes
Configuration en interface graphique
Les test de vies et vérification
TP : Mise en place d'un load balancing HTTP/HTTPS

ACCESS POLICY MANAGER

Concept
Mode de déploiement
Fonctionnalités
Visual policy Editor

ACCÈS DISTANT : PORTAIL SSL

Publication de serveur
Authentification
Étapes de mise en place
TP : Configuration d'un accès distant via un portail SSL

ACCÈS DISTANT : TUNNELING SSL

Concepts
Edition d'un politique
Authentification
TP : Configuration d'un accès distant SSL test

SE 315

LE HACKING - COMMENT SE PROTÉGER DU PIRATAGE INFORMATIQUE

OBJECTIFS

Cette formation sécurité informatique a pour but de vous montrer la démarche des pirates, leur méthodologie ainsi que les outils qu'ils utilisent. Ainsi vous serez sensibilisé aux faiblesses de votre Système d'Information et vous serez à même de mettre en place les parades pour en réduire les vulnérabilités.

PUBLIC

Décideur, architecte, administrateur réseau et systèmes concernés par les problèmes de sécurité, responsable de l'audit informatique, chef de projet informatique

PRÉREQUIS

Connaissance des réseaux, des bases du chiffrement et du filtrage pour les personnes impliquées dans la SSI : RSSI, Ingénieurs/Techniciens/Administrateurs système et réseau.

2 JOURS

POINTS CLÉS DU PROGRAMME

INTRODUCTION

La structure du système d'information et les menaces
La démarche sécurité
L'aspect «politique»
L'aspect «technique»
L'aspect juridique
Le monde du piratage

LA MÉTHODOLOGIE D'ATTAQUE

Les étapes d'une intrusion

L'EXPLOITATION D'ATTAQUE

La collecte d'informations sur la cible

LE NIVEAU RÉSEAU

Les accès aux composants du réseau Telnet, le vol de mot de passe, injection de commandes SHT (SCP sftp)
Les switch
L'écoute du trafic par attaque du switch
Les routeurs points d'accès WiFi
Les périphériques bluethooth
Le PABX et la VoIP /ToIP
L'écoute téléphonique

LE NIVEAU DU SYSTÈME D'APPLICATIONS

Le piratage du système d'exploitation
Le BIOS
Les chevaux de Troie et les portes dérobées
Cas pratiques et exemples
Les atteintes à la disponibilité
Les classiques
L'utilisation des bugs
Les vulnérabilités des applications web
Les vulnérabilités côté serveurs
Les attaques côté serveur
Les attaques côté client
Les vulnérabilités de la messagerie
Les atteintes à la disponibilité
L'introduction d'un vers et/ou d'un virus dans le SI
Atteinte à la confidentialité, disponibilité, intégrité

LE CONTOURNEMENT D'OUTILS DE SÉCURITÉ

Coupe-feu, système d'IDS, pot de miel
Contournement d'antivirus, l'effacement des logs

SYNTHÈSE

La gestion des mises à jour
La veille technologique
Les liens web utiles pour la sécurité

SE 316

DÉTECTER UNE INTRUSION DANS SON SI

OBJECTIFS

Cette formation à la fois théorique et pratique présente les techniques d'attaques les plus évoluées à ce jour et montre comment y faire face. À partir d'attaques réalisées sur cibles identifiées (serveurs Web, clients, réseaux, firewall, bases de données...), le participant apprendra à déclencher la riposte adaptée (filtrage d'anti-trojan, filtrage URL mal formée, détection de spam et détection d'intrusion en temps réel avec sonde IDS).

PUBLIC

Ingénieurs sécurité, système et réseau ayant à sécuriser le SI de l'entreprise. Chefs de projets souhaitant comprendre les attaques auxquelles l'entreprise est confrontée et mettre en œuvre les meilleures riposte technologiques.

PRÉREQUIS

Bonnes connaissances des réseaux TCP/IP. Connaissances de base en sécurité informatique.

4 JOURS

POINTS CLÉS DU PROGRAMME

LE MONDE DE LA SÉCURITÉ INFORMATIQUE

Définitions «officielles» : le hacker, le hacking
La communauté des hackers dans le monde, les «gurus», les «script kiddies»
L'état d'esprit et la culture du hacker
Les conférences et les sites majeurs de la sécurité

TCP/IP POUR FIREWALLS ET DÉTECTION D'INTRUSIONS

IP, TCP et UDP sous un autre angle
Zoom sur ARP et ICMP
Le routage forcé de paquets IP (source routing)
La fragmentation IP et les règles de réassemblage
De l'utilité d'un filtrage sérieux
Sécuriser ses serveurs : un impératif
Les parades par technologies du routeur filtrant au firewall stateful inspection ; du proxy au reverse proxy
Panorama rapide des solutions et des produits
Travaux pratiques

COMPRENDRE LES ATTAQUES SUR TCP/IP

Le «Spoofing» IP
Attaques par déni de service
Prédiction des numéros de séquence TCP
Vol de session TCP : Hijacking (Hunt, Juggernaut)
Attaques sur SNMP
Attaque par TCP Spoofing (Mitnick) : démystification
Travaux pratiques

INTELLIGENCE GATHERING : L'ART DU CAMOUFLAGE

Chercher les traces : interrogation des bases WHOIS, les serveurs DNS, les moteurs de recherche
Identification des serveurs
Comprendre le contexte : analyser les résultats, déterminer les règles de filtrage, cas spécifiques
Travaux pratiques

PROTÉGER SES DONNÉES

Systèmes à mot de passe «en clair», par challenge, crypté
Le point sur l'authentification sous Windows
Rappels sur SSH et SSL (HTTPS)
Sniffing d'un réseau switché : ARP poisonning
Attaques sur les données cryptées : «Man in the Middle» sur SSH et SSL, «Keystoke Analysis» sur SSH
Détection de sniffer : outils et méthodes avancées
Attaques sur mots de passe
Travaux pratiques

DÉTECTER LES TROJANS ET LES BACKDOORS

État de l'art des backdoors sous Windows et Unix
Mise en place de backdoors et de trojans
Le téléchargement de scripts sur les clients, exploitation de bugs des navigateurs
Les «Covert Channels» : application client-serveur utilisant ICMP (Loki), communication avec les agents de déni de services distribués
Travaux pratiques

DÉFENDRE LES SERVICES EN LIGNE

Prise de contrôle d'un serveur : recherche et exploitation de vulnérabilités, mise en place de «backdoors» et suppression des traces. - Comment contourner un firewall ? (netcat et rebonds.)
La recherche du déni de service
Les dénis de service distribués (DDoS)
Les attaques par débordement (buffer overflow). Exploitation de failles dans le code source.
Techniques similaires : «Format String», «Heap Overflow»…
Vulnérabilités dans les applications Web
Vol d'informations dans une base de données
Les RootKits
Travaux pratiques

COMMENT GÉRER UN INCIDENT ?

Les signes d'une intrusion réussie dans un SI
Qu'ont obtenu les hackers ? Jusqu'où sont-ils allés ?
Comment réagir face à une intrusion réussie ?
Quels serveurs sont concernés ?
Savoir retrouver le point d'entrée… et le combler
La boîte à outils Unix/Windows pour la recherche de preuves
Nettoyage et remise en production de serveurs compromis

CONCLUSION : QUEL CADRE JURIDIQUE ?

La réponse adéquate aux hackers
La loi française en matière de hacking
Le rôle de l'état, les organismes officiels
Qu'attendre de l'Office Central de Lutte contre la Criminalité (OCLCTIC) ?
La recherche des preuves et des auteurs
Et dans un contexte international ?
Le test intrusif ou le hacking domestiqué ?
Rester dans un cadre légal, choisir le prestataire, être sûr du résultat

Frame IP Formation

SE 317

RÉALISER UN AUDIT DE SÉCURITÉ INFORMATIQUE

OBJECTIFS

- Identifier les failles intrinsèques aux protocoles utilisés sur les systèmes d'information
- Identifier les menaces
- Comprendre ce qu'est le «social engineering»
- Comprendre les pratiques des normes ISO 27000
- Comprendre la modélisation COBIT
- Choisir les outils adéquats pour un audit sécurité
- Exécuter l'audit
- Analyser les résultats de l'audit
- Choisir les méthodes de changement nécessaires, suite à l'audit
- Établir des rapports d'audit sécurité

PUBLIC

Toute personne en charge de la sécurité d'un système d'information ou intervenant, RSSI.

PRÉREQUIS

Savoir utiliser un système d'exploitation (Linux ou Microsoft).
Avoir des notions sur TCP/IP.
Connaître les rôles des différents dispositifs réseau.

4 JOURS

POINTS CLÉS DU PROGRAMME

INTRODUCTION

Principes des audits informatiques
Rôle du système d'information
Les Télécommunications
Gestion des projets informatiques
Concepts du COBIT
Modélisation COBIT
Présentation de la norme ISO 27000
Norme 27001 : exigences
Norme 27002 : bonnes pratiques
Norme 27007 : guide pour l'audit
Les documentations à tenir

LES ÉLÉMENTS D'UN SYSTÈME D'INFORMATION

Les stations finales
Les serveurs
Les routeurs
Les commutateurs
Les équipements WiFi
Les firewalls
Les antivirus
Les spywares
Les applications
Les dispositifs connectables
Les utilisateurs

PRÉPARER UN AUDIT DE SÉCURITÉ

Évaluation de l'existant au niveau architecture
Les normes
Les failles connues
Sécurité physique
Sécurité logicielle
Les éléments critiques de l'infrastructure
Définition des pôles d'activité de l'entreprise
Détermination des risques
Calcul des coûts d'un incident
Définition des groupes d'utilisateurs ou des groupes métiers
Préparation d'interviews des utilisateurs clés
Mise en place des questionnaires
Adaptation du langage selon les acteurs audités
Lisibilité des rapports

CHOIX DES MÉTHODES ET DES OUTILS

Les tests de techniques
Processus de contrôle
Rédaction des tableaux de bord
Choisir des indicateurs quantifiables
Choix des cibles de l'audit
Définition du périmètre de l'audit
Suivi des référentiels ISO, COBIT et ITIL
Protection des personnes
Protection des biens
Protection des ressources immatérielles

CONCLUSION DE L'AUDIT

Définition des objectifs
Rédaction d'un tableau de bord
Préconisations
Élaboration de tableaux de calculs
Présentation du retour sur investissement
Définition d'un plan de continuité d'activité
Définition d'un plan de reprise d'activité

Tallen Si Formation

SE 318

SÉCURISER UN SYSTÈME LINUX

OBJECTIFS

- Comprendre comment bâtir une sécurité forte autour de Linux
- Savoir mettre en place la sécurité d'une application Linux
- Comprendre les fondamentaux de la sécurité informatique et notamment de la sécurité réseau
- Être capable de sécuriser les échanges réseaux en environnement hétérogène grâce à Linux

PUBLIC

Administrateurs Linux, les ingénieurs système, architectes réseaux et consultants sont aussi des candidats appropriés pour cette formation.

4 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

LES ENJEUX DE LA SÉCURITÉ

Les attaques, les techniques des hackers
Panorama des solutions
La politique de sécurité

LA CRYPTOLOGIE OU LA SCIENCE DE BASE DE LA SÉCURITÉ

Les concepts de protocoles et d'algorithmes cryptographiques
Les algorithmes symétriques et asymétriques (à clé publique), les fonctions de hachage
La signature numérique, les certificats X-509, la notion de PKI

LES UTILISATEURS ET LES DROITS

Rappels sur la gestion des utilisateurs et des droits, les ACLs
La dangerosité des droits d'endossement
La sécurité de connexion, le paquetage SHADOW

LES BIBLIOTHÈQUES PAM

L'architecture du système PAM, les fichiers de configuration
L'étude des principaux modules

LES PRINCIPAUX PROTOCOLES CRYPTOGRAPHIQUES EN CLIENT/SERVEUR

SSH, le protocole et les commandes ssh
SSL, l'utilisation de SSL et des certificats X-509 dans Apache et stunnel
Kerberos et les applications kerbérorérisées

LES PARE-FEUX

Panorama des techniques pare-feux
L'architecture Netfilter/Iptables, la notion de chaine, la syntaxe d'iptables
La bibliothèque tcpd ou l'enveloppe de sécurité, la sécurisation via xinetd
Mise en place d'un routeur filtrant, du masquerading et d'un bastion avec iptables
Le proxy SQUID

LES VPN

Panorama des techniques tunnels et VPN
Le logiciel OpenVPN

LA SÉCURISATION DES APPLICATIONS

Principes généraux
Sécurisation du Web, d'email, du DNS, du FTP

LES TECHNIQUES D'AUDIT

L'audit des systèmes de fichiers avec Tripwire
Les outils d'attaque réseau
La détection des attaques avec snort

Frame IP Formation

Tallen Si Formation

COMMUNICATIONS UNIFIÉES

COM 401	Introduction à la ToIP d'entreprise
COM 402	Asterisk - Les fondamentaux
COM 403	Asterisk - L'expertise
COM 404	Configuration et administration d'une infrastructure Cisco Call Manager
COM 405	Comprendre et gérer son architecture Cisco Call Manager
COM 406	Approche technique de la visioconférence
COM 407	Expertise protocolaire sur la visioconférence
COM 408	La visioconférence
COM 409	Implémentation et planification de Microsoft Lync Server

La téléphonie sur IP est un service de téléphonie fourni sur un réseau de télécommunications ouvert au public ou privé utilisant principalement le protocole de réseau IP.

La téléphonie sur IP peut :

- Se rajouter en complément sur un réseau téléphonique traditionnel existant avec une passerelle
- S'utiliser en full-IP pour une nouvelle infrastructure
- S'utiliser en multi sites full IP avec l'aide d'un opérateur adéquat et parfois des serveurs centralisés
- S'utiliser sur un ordinateur relié au réseau Internet à destination d'un autre ordinateur relié lui aussi au réseau Internet, mais en utilisant absolument le même logiciel (les communications seront donc gratuites de PC à PC).

Nous vous permettons de découvrir et de prendre en main la téléphonie sur IP afin de garantir à votre entreprise un service de téléphonie moins onéreux, plus souple et porté vers l'avenir.

COM 401

INTRODUCTION À LA TOIP D'ENTREPRISE

OBJECTIFS

Cette formation est une introduction à la ToIP dans le but de découvrir la téléphonie sur IP de manière générale.

PUBLIC

Administrateur

1 JOUR

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION
- Les objectifs du cours
- L'intérêt de la ToIP

PRÉSENTATION DE LA TOIP
- Qu'est-ce que la VoIP et la ToIP ?
- Les problématiques
- Les fondamentaux
- Les périmètres VoIP et ToIP
- Les enjeux et avantages
- Les contraintes

ÉTAT DE L'ART DE LA TOIP
- Le marché
- Les solutions
- Les acteurs

LES PROTOCOLES

LES PROTOCOLES DE SIGNALISATION LIBRES

LES PROTOCOLES DE SIGNALISATION PROPRIÉTAIRES

LES PROTOCOLES DE TRANSPORT

LES CODECS

LA QUALITÉ DE SERVICE

LES SERVICES
- Les services traditionnels
- Les services avancés

LES ÉQUIPEMENTS
- Les IPBX
- Les passerelles
- Les boitiers de conversion
- Le réseau
- Les téléphones IP

L'ARCHITECTURE
- Architecture standard
- Architecture avancée
- Architecture « Centrex IP »
- Architecture convergente
- La voix sur WiFi
- La sécurité

LA MIGRATION
- Le plan de numérotation
- La conduite du changement
- La migration « Tdm » vers l'IP
- Les stratégies de migration
- Les bonnes pratiques

COM 402

ASTERISK - LES FONDAMENTAUX

OBJECTIFS

- Maîtriser les différents concepts propres à la voix sur IP
- Être capable de mettre en place une solution de voix sur IP
- Installer et configurer la solution de voix sur IP Open Source Asterisk
- Acquérir les bonnes pratiques pour mettre en place une solution de voix sur IP

PUBLIC

Techniciens mainteneurs d'IPBX, Consultants en technologie réseau, chefs de projets techniques.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

RAPPELS SUR LA TOIP/VOIP
- Qu'est-ce que la VoIP et la ToIP ?
- État de l'art ToIP
- Les 5 axes de la ToIP
- ToIP vs VoIP
- Les avantages, les enjeux
- Les acteurs : équipementiers, standardisation, régulation, opérateurs et fournisseurs de services

PRÉSENTATION DU PRODUIT ASTERISK-DIGIUM
- Présentation de l'Open Source
- Historique d'Asterisk
- Concepts de base (principes de base, composantes et architectures)
- Les protocoles Asterisk : IAX-IAX2, H323, MGCP, SIP, Zap, SS7, RTP et RTCP
- Codage et codecs

MISE EN ŒUVRE PRATIQUE
- Les équipements (serveur, cartes, téléphones, boitier ATA)
- Gateway, boitiers ATA, équipements réseaux, postes IP
- Les fichiers et leur emplacement entrant dans la configuration de base d'Asterisk
- Ajouter/modifier/supprimer des utilisateurs avec SIP et IAX2
- Installer/configurer/exploiter des cartes de liaison extérieures
- Le routage des utilisateurs au sein du système
- Administration des différents niveaux d'accès selon les utilisateurs
- Administration et débuggage d'Asterisk (en utilisant la CLI)
- Sécurisation du système

LES SERVICES
- Ajouter/modifier/supprimer des services sur Asterisk
- Les services : Présentation, boîte vocale, files d'attente, Click to dial,
- Personnalisation du téléphone, T9, Messagerie intégrée, Messagerie unifiée, Annuaire d'entreprise (unifié),
- SVI (Serveur vocal interactif), «Free Seating», gestion de présence, conférences vocales/vidéos/données,
- Messagerie instantanée, Softphones, etc.… synthèse

ÉVOLUTION ET MIGRATION
- Évolutions possibles (partage de la communauté, la convergence)
- La conduite de changement
- Ce qu'il faut retenir :
- La démarche et la structure d'un projet de migration
- Liens/sources
- Fonctionnement basique des flux d'appels

COM 403

ASTERISK - L'EXPERTISE

OBJECTIFS

- Maîtriser les différents concepts propres à la voix sur IP
- Être capable de mettre en place une solution de voix sur IP
- Installer et configurer la solution de voix sur IP Open Source Asterisk
- Acquérir les bonnes pratiques pour mettre en place une solution de voix sur IP

PUBLIC

Techniciens mainteneurs d'IPBX, consultants en technologie réseau, chefs de projets techniques.

5 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION À LA TÉLÉPHONIE SUR IP

Le marché de la voix sur IP
Les différentes solutions existantes
Les enjeux de la voix sur IP
Comprendre le protocole VoIP
Comprendre les codecs et le «transcoding»

CONCEPTS AVANCÉS DE VOIX SUR IP

Configurer des terminaisons VoIP
Théorie sur SIP
Théorie sur IAX
Gérer les réseaux, les pare-feux et les NAT
Latence, Jitter, bande passante et overhead IP

PRÉSENTATION D'ASTERISK PBX OPEN SOURCE

Comprendre ce qu'est Asterisk et son utilité
Comprendre la licence Open Source d'Asterisk
L'architecture Asterisk

INSTALLATION ET DÉMARRAGE D'ASTERISK

Les différents mécanismes d'installations d'Asterisk
Charger et configurer les drivers Zaptel
Les différentes méthodes pour démarrer Asterisk

CONFIGURER UN PBX BASIQUE

Fonctionnement basique des flux d'appels
Ajout d'extensions et de périphériques
Les fichiers de configuration Asterisk
Mise en place d'un PBX simple avec deux stations

LES DIALPLAN ASTERISK

Comprendre ce qu'est un dialplan
Mise en place des fondations d'un PBX fonctionnel
Mettre en place des dialplans interactifs avec des applications avancées
Réaliser des menus vocaux
Mettre en place des boîtes vocales

PROGRAMMER DES FONCTIONS AVANCÉES

Utiliser des fonctions de dialplan et accroître la puissance d'Asterisk
Mettre ensemble des expressions, variables et fonctions pour créer des branches conditionnelles et des boucles
Utiliser les macros pour simplifier un dialplan
Configurer Asterisk pour les SDA
Utiliser des fichiers d'appel pour automatiser les appels téléphoniques

CONNECTER ASTERISK AU RTC

Les différents ports utilisés (FXS, FXO, ...)
Les différents types de signalling analogique disponibles sur Asterisk
Installer et configurer les interfaces analogiques et les pilotes d'interfaces dans Asterisk

GÉRER LES FILES D'ATTENTE

Les files d'attente, les agents
Exemples d'utilisation
Création d'un centre d'appel

NOTIONS AVANCÉES DE LA TÉLÉPHONIE SUR IP AVEC ASTERISK

Debugger son système Asterisk
Téléphonie numérique avec Asterisk
Écrire un programme AGI simple
Asterisk Manager Interface (AMI) - Asterisk Realtime Architecture (ARA)
Routage des appels entrants

COM 404

CONFIGURATION ET ADMINISTRATION D'UNE INFRASTRUCTURE CISCO CALL MANAGER

OBJECTIFS

- Dimensionner son infrastructure réseau afin d'accueillir un Call Manager
- Installer et gérer les composants Call Manager
- Concevoir un dial plan
- Configurer une solution complète VoIP Cisco

PUBLIC

Achitecte, administrateurs, consultants et ingénieurs réseaux

PRÉREQUIS

Connaissances de base en réseau. Connaissances des éléments d'une achitecture Call Manager Cisco

5 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION

Solution Cisco
Composants de la gamme
Gestion des licences

DESIGN LAN ET WAN

Concevoir et dimensionner son LAN
Dimensionnement WAN
Implémentation d'une QoS basique
Signalisation et flux voix

DESIGN ET ARCHITECTURE

Design mono, multi site, centralisé ou distribué
Architecture en cluster
Installation des composants
Présentation des interfaces administrateur
TP : Utilisation de Prime Collaboration Deployment

GESTION DES UTILISATEURS

Synchronisation avec les annuaires LDAP / Active Directory / Domino
Création individuelle ou en masse des utilisateurs
TP : création d'un annuaire call manager

ROUTAGE DES APPELS

Introduction à la gamme des téléphones IP Cisco
Passerelles voix et Trunk SIP
Les composants d'un plan de numérotation

DIAL PLAN AVANCÉ

Présentation des Calling Search Space et Partitions pour gérer les restrictions d'appel
Conception d'un dial plan cohérent
TP : création d'un dial plan

GESTION DES SERVICES TÉLÉPHONIQUES

Gestion des groupements et files d'attente
Serveur vocal interactif
Musique d'attente
TP : configuration de services

GESTION DES SERVICES UTILISATEURS

Modèle de Softkey
Services de bases : interception d'appel, speed dial, supervision
Paramétrage par l'interface web utilisateur
TP : configuration et personnalisation d'un téléphone Cisco

DÉPLOIEMENT ET PROVISIONNING

Configuration de l'infrastructure LAN pour alimenter les téléphones et leur affecter un VLAN
Configuration DHCP et TFTP
Provisionning manuel
Autoprovisionning par synchronisation LDAP automatique
Self provisionning utilisateur
TP : provisionning d'un téléphone Cisco

GESTION DE LA MOBILITÉ

Introduction du principe de profil itinérant
Configuration d'un profil
Gestion externe de la mobilité
TP : Configuration d'un profil itinérant

INTÉGRATION DE CISCO UNITY

Gestion des utilisateurs et boites vocales
Intégration de Unity à un CUCM
Unification avec Microsoft Exchange
TP : configuration d'un serveur Unity

COM 405

COMPRENDRE ET GÉRER SON ARCHITECTURE CISCO CALL MANAGER

OBJECTIFS

- Identifier les éléments d'une infrastructure CUCM
- Dimensionner et concevoir une architecture voix
- Choisir le modèle de déploiement et de redondance dans le cluster le plus approprié
- Installer et gérer les serveurs de l'infrastructure

PUBLIC

Architectes, administrateurs, consultants et ingénieurs réseaux

3 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION À LA TOIP

- Solution Cisco
  - Equipements Voix
  - IP Phone et visioconférence
- Design LAN et WAN

PRÉSENTATION DE LA SOLUTION CUCM

- Composants de la gamme
- Evolution des fonctionnalités des versions 9 et 10
- Nouveauté Jabber
- Migration et upgrade

ARCHITECTURE

- Design mono, multi site, centralisé ou distribué
- Architecture en cluster
- Protocoles de signalisation SIP et SCCP

ADMINISTRATION

- Prime Collaboration Deployment (PCD)
- Cisco Unified Communication Manager
- Cisco Unified Presence Software
- Cisco Unity

INTERFACE UTILISATEUR

- Annuaire et préférences utilisateur
- Gestion du téléphone

INSTALLATION D'UN CALL MANAGER V10 BASIQUE

- Utilisation de Prime Collaboration Deployment
- Installation d'un CUCM
- Installation d'un serveur de messagerie
- TP : Utilisation de Prime Collaboration Deployment

INITIATION À LA CONFIGURATION

- Annuaire et gestion des utilisateurs
- Gestion des Terminaux IP
- Passerelles voix et Trunk SIP
- Routage des appels
- TP : configuration basique d'un téléphone

COM 406

APPROCHE TECHNIQUE DE LA VISIOCONFÉRENCE

OBJECTIFS

L'objectif de cette formation est de vous présenter toutes les technologies relatives à la visioconférence. En dressant un portrait technique et fonctionnel, cette formation vous permettra de prendre de la hauteur sur vos projets afin d'optimiser les performances visio.

PUBLIC

Public débutant possédant des connaissances de base en informatique

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

INTRODUCTION ET RAPPELS

- Qu'est-ce que la visio ?
- Les avantages de la visio
- Les supports de la visio
  1. RNIS
  2. IP (LAN)
  3. Internet (Skype)
  4. Les normes et protocoles
- Les Codecs

LES FLUX VISIO

- Flux Audio (Nature, BP consommée, technologie utilisée...)
- Flux Vidéo (Nature, BP consommée, technologie utilisée...)
  1. Qualité HD, Full HD
  2. Bande passante minimale
  3. Dégradation de qualité
- Communication point à point
- Communication multipoint (MCU…)
- Les différents types de visioconférence (téléprésence, web conférence…)

INTÉGRATION AU SEIN DU RÉSEAU

- Parallèle avec la Téléphonie
- Les flux : Notion de QoS

LES PASSERELLES

- Quelques exemples de câblages / débits…

LA SÉCURITÉ

- Sécurisation de l'ordinateur
- Franchissement des firewalls
- Les gatekeeper

LES ÉQUIPEMENTS DE VISIOCONFÉRENCE

- Les différents constructeurs
- Quelques exemples de kits constructeurs
- Les meubles
- Les salles visio

TP : DÉMONSTRATION AVEC PLUSIEURS PRODUITS

COM 407

EXPERTISE PROTOCOLAIRE SUR LA VISIOCONFÉRENCE

OBJECTIFS

- Comprendre les mécanismes de fonctionnement de la visioconférence
- Avoir un panel des codecs à mettre en place
- Appréhender les contraintes sur l'architecture réseau
- Incorporer la sécurité

PUBLIC

Administrateur

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

LA VISIOCONFÉRENCE

Définitions et enjeux
Domaines d'application (formation/réunion/optique green it/e-learning/ …)
Principales technologies
Les fournisseurs

L'ARCHITECTURE

Le Manager (gatekeeper)
Le Pont de visioconférence (MCU)
L'enregistreur
Les terminaux (endpoints)

LE PROTOCOLE H.323

Présentation
La pile protocolaire
La signalisation (H.225 RAS et H.225 Call Signaling)
La négociation de codecs (H.245)
Le transport de l'information (RTP et RTCP)
Déroulement d'un appel
TP : suivre les différentes phases d'établissement d'un appel à l'aide de wireshark

LES CODECS

Codecs audio/Famille G.7xx
Codecs vidéo/Famille H.26x

RÉSEAU

Les contraintes
Ressources nécessaires (débit + latence + perte de paquets + gigue)
La qualité de service
Traversée des firewalls/NAT
Le protocole H.460.18

SÉCURITÉ

Sécurisation de l'architecture
Contexte (problématique sur les ports négociés dynamiquement)
Filtrage réseau par ACL pour les équipements H.323
Proxy H.323 derrière un firewall
Firewall State Full inspection
Sécurisation des appels
Le protocole H.235

COM 408

LA VISIOCONFÉRENCE

OBJECTIFS

Cette formation est destinée à vous faire découvrir le monde de la visioconférence et vous apporter tous les éléments pour vous permettre de démarrer vos projets sur des bases saines et clairement définies.

PUBLIC

Public débutant possédant des connaissances de base en informatique

1 JOUR

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

QU'EST-CE QUE LA VISIO ?

Définition de la visioconférence
Un bref historique
Évolutions à venir
État du marché

PRÉSENTATION DES PRINCIPALES TECHNOLOGIES

La visioconférence par IP
La visioconférence par ligne RNIS
La visioconférence par réseau 3G
Avantages/Inconvénients de chaque solution

LES TYPES DE VISIOCONFÉRENCES

La téléprésence
La visioconférence de salle
La visioconférence par Webcam
La visioconférence de bureau
Location de salles de visioconférence

LES SERVICES

Les outils collaboratifs
Les outils de management

LES DIFFÉRENTS CONSTRUCTEURS ET LEURS PRODUITS

Polycom
Cisco
Radvision
LifeSize
Sony

DÉMONSTRATION D'UNE OU PLUSIEURS SOLUTIONS DE VISIOCONFÉRENCE

COM 409

IMPLÉMENTATION ET PLANIFICATION DE MICROSOFT LYNC SERVER

OBJECTIFS

- Savoir mettre en place la solution de communication unifiée de Microsoft : Lync Server
- Être en mesure de préparer, configurer et déployer les fonctionnalités de base du module de téléphonie de Lync Server
- Être capable de configurer l'interopérabilité entre Lync Server et Exchange
- Comprendre comment configurer et gérer les conférences
- Savoir sauvegarder et restaurer les données critiques de Lync Server

PUBLIC

Professionnels des systèmes informatiques et professionnels des systèmes de télécommunications. Toute personne en charge du déploiement et de l'administration d'une solution reposant sur Lync Server.

PRÉREQUIS

- Avoir une bonne connaissance des concepts de téléphonie : TDM, VoIP, passerelles, PBX, SIP, codecs...
- Avoir les connaissances de base sur TCP/IP, Windows Server 2008, AD, PKI, Exchange, PowerShell et SQL server
- Une première expérience de Microsoft Lync Server est vivement conseillée pour suivre cette formation

5 JOURS

POINTS CLÉS DU PROGRAMME

FONCTIONNALITÉS ET CONCEPTION D'ARCHITECTURE MICROSOFT LYNC SERVER

- Fonctionnalités de Lync Server
- Présentation de l'architecture
- Architecture et rôles des serveurs
- Outils d'administration

CONCEPTION DE LA TOPOLOGIE LYNC SERVER

- Planification de l'infrastructure Lync
- Utilisation de «Lync Server Planning Tool»
- Utilisation de «Topology Builder»
- Planification de l'infrastructure serveur
- Conception de la documentation

CONFIGURATION DES UTILISATEURS ET DE LEURS DROITS DANS MICROSOFT LYNC SERVER

- Gestion de Lync Server
- Introduction au contrôle des accès basés sur les rôles

DÉPLOIEMENT ET GESTION DES CLIENTS ET PÉRIPHÉRIQUES

- Préparation du déploiement des clients
- Déploiement des clients Lync
- Préparation du déploiement des périphériques
- Déploiement et gestion des téléphones IP

CONFÉRENCE AVEC LYNC SERVER

- Introduction à la conférence dans Lync Server
- Configuration des conférences Audio, Vidéo et Web
- Conférence Dial-In dans Lync Server
- Gestion et administration des stratégies de conférence

CONCEPTION ET DÉPLOIEMENT DES ACCÈS EXTERNES

- Les possibilités offertes par Lync Server
- Planifier la messagerie instantanée et la fédération de présence
- Conception des services

DÉPLOYER LE SERVICE DE CHAT PERSISTANT

- Vue d'ensemble de l'architecture
- Conception du service
- Déploiement et configuration

SURVEILLANCE ET ARCHIVAGE

- Description du service d'archivage
- Description du service de surveillance
- Configuration de l'archivage et de la surveillance

ADMINISTRATION ET MAINTENANCE DE LYNC SERVER

- Introduction aux outils de dépannage de Lync Server
- Comprendre ce que sont les tâches opérationnelles
- Les différentes techniques de dépannage de Lync Server
- Introduction à l'analyse des fichiers de logs et des traces

HAUTE DISPONIBILITÉ DANS MICROSOFT LYNC SERVER

- Configuration de la Haute Disponibilité dans Lync Server
- Planification de la mise en oeuvre du Load Balancing
- Conception du Load Balancing

RÉCUPÉRATION D'URGENCE DANS MICROSOFT LYNC SERVER

- Les outils de sauvegarde et de récupération de Lync Server
- Les données critiques de Lync Server à sauvegarder et restaurer
- Les données critiques de Lync Server à importer et exporter
- Conception de la résilience de sites

PLANIFICATION DE LA MIGRATION VERS LYNC SERVER

- Vue d'ensemble de la coexistence et de la migration
- Les étapes de la migration
- Planification de la migration des clients et des périphériques
- Stratégie de migration

SYSTÈME

Nouvelle interface d'administration, évolution des serveurs, virtualisation, stockage, le cloud sont autant de raisons, parmi bien d'autres, qui vont très certainement amener les DSI à évoluer vers de nouveaux usages et ceci est d'autant plus probable que la majorité des serveurs d'entreprise fonctionne encore avec d'anciennes version d'OS.

Alors va irrémédiablement se poser la question des compétences disponibles pour mettre en oeuvre et administrer des solutions qui ont considérablement évoluées.

Les cursus de formation s'adressent aux professionnels amenés à implémenter et à assurer l'administration des éléments du SI, de l'installation jusqu'à la mise en oeuvre de fonctionnalités avancées.

SYS 501

L'ESSENTIEL DES BASES DE DONNÉES

OBJECTIFS

- Disposer d'une vision claire de ce qu'est un SGBD
- Comprendre l'intérêt de modéliser correctement une base de données pour garantir l'intégrité et les performances
- Découvrir la puissance du langage SQL pour manipuler les données
- Identifier les principaux acteurs du marché ainsi que les forces et faiblesses de leurs solutions

PUBLIC

Utilisateurs d'outils décisionnels et toute personne désirant comprendre le monde des bases de données.

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

HISTORIQUE
- Le «tout fichier»
- Le besoin de centraliser les traitements des fichiers
- L'avènement des systèmes de gestion centralisés
- L'externalisation des processus métiers
- Le client-serveur applicatif

LE SYSTÈME DE GESTION DE BASES DE DONNÉES
- Les briques constitutives
- Le(s) langage(s) de requêtage
- Les contraintes d'utilisation

LA MODÉLISATION DES DONNÉES
- Besoin de normalisation
- Modèles conceptuels
- Modèle physique
- Les relations et leurs éléments
- Les limites de Merise

TYPES DE SGBD
- Les SGBD relationnels
- Les SGBD objets
- Place de XML/XSL

ADMINISTRATION DES SGBD
- Un besoin fondamental
- La sécurité des données
- Réplication ou répartition ?
- Les grappes de SGBD

LES ACTEURS
- Les professionnels : Oracle, SQL Server, IBM DB2
- Les puissants : MySQL, PostgreSQL
- Comment choisir son SGBD ?

PRÉSENTATION DES LANGAGES DE REQUÊTAGE
- SQL du monde relationnel
- OQL de EyeDB

ÉTAT DE L'ART
- Les 'grilles' de SGBD
- Les proxy de SGBD
- XSQL

SYS 502

ADMINISTRER ET MAINTENIR UNE BASE DE DONNÉES

OBJECTIFS

- Connaître de façon approfondie les fonctionnalités d'un SGBD, son architecture technique, ses concepts et ses mécanismes
- Savoir créer une base de données et réaliser les principales opérations d'administration de base
- Être en mesure de gérer la sécurité sur les objets des bases

PUBLIC

Administrateurs de bases de données et chefs de projet

5 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

PRÉSENTATION DE L'ARCHITECTURE

LA BASE DE DONNÉES

LES STRUCTURES GLOBALES DE STOCKAGE

LA GESTION AUTOMATIQUE DE LA MÉMOIRE

LES UTILISATEURS ET LEURS DROITS

LE STOCKAGE D'UN SCHÉMA APPLICATIF

LES UTILITAIRES ET LES SAUVEGARDES

SYS 503

ASSURER LE DÉPLOIEMENT ET LE SUPPORT DU POSTE DE TRAVAIL WINDOWS

OBJECTIFS

- Savoir détecter et résoudre les problèmes de compatibilité applicative
- Disposer des clés pour le choix d'une méthode de déploiement adaptée au contexte
- Savoir créer des images de référence pour un déploiement par clonage
- Connaître et maîtriser les outils de déploiement et leur domaine d'applicabilité
- Être à même de prendre en charge le transfert des données et paramètres utilisateurs lors de la migration
- Être en mesure de définir et optimiser l'environnement client

PUBLIC

Toute personne en charge du déploiements Windows 7

PRÉREQUIS

- Connaissance du poste de travail Windows
- Connaissances de base sur TCP / IP

5 JOURS

POINTS CLÉS DU PROGRAMME

PRÉPARATION AU DÉPLOIEMENT DE POSTES DE TRAVAIL WINDOWS

Présentation du cycle de vie des postes de travail
Déploiement des postes de travail : défis et considérations
Outils et technologies utilisés dans le cycle de vie du déploiement de postes de travail
Évaluation de l'environnement informatique actuel en vue du déploiement de Windows
Conception de l'activation de Windows

ÉVALUATION DE LA COMPATIBILITÉ DES APPLICATIONS SOUS WINDOWS

Vue d'ensemble de la compatibilité des applications
Identification et résolution des problèmes de compatibilité des applications à l'aide d'ACT

ÉVALUATION DES MÉTHODES DE DÉPLOIEMENT DE WINDOWS

Évaluation du déploiement sur place
Évaluation du déploiement côte à côte
Évaluation de la méthode de déploiement Lite Touch
Évaluation de la méthode de déploiement Zero Touch

CONCEPTION D'IMAGES STANDARDS DE WINDOWS

Vue d'ensemble de l'architecture d'installation Windows
Vue d'ensemble du processus de création d'image
Élaboration de la stratégie relative aux images
Sélection des méthodes de maintenance d'images

DÉPLOIEMENT DE WINDOWS À L'AIDE DU KIT WINDOWS ADK

Présentation de l'outil D'ADK
Création d'une image de référence Windows
Gestion de l'environnement de préinstallation Windows
Capture, application et maintenance d'une image Windows

DÉPLOIEMENT DE WINDOWS À L'AIDE DES SERVICES DE DÉPLOIEMENT

Présentation des services WDS
Conception et configuration des services WDS pour le déploiement de Windows

DÉPLOIEMENT DE WINDOWS À L'AIDE DE LITE TOUCH INSTALLATION

Conception de l'environnement d'installation LTI (Lite Touch Installation)
Implémentation de MDT pour le déploiement de Windows

DÉPLOIEMENT DE WINDOWS À L'AIDE DE ZERO TOUCH INSTALLATION

Conception de l'environnement ZTI (Zero Touch Installation)
Installation ZTI de Windows à l'aide d e MDT et de Configuration Manager

MIGRATION D'UTILISATEURS AVEC L'OUTIL DE TRANSFERT WINDOWS ET L'OUTIL USMT

Présentation de la migration des utilisateurs
Présentation de l'outil USMT
Planification de la migration des utilisateurs
Migration des utilisateurs avec l'outil USMT

CONCEPTION, CONFIGURATION ET GESTION DE L'ENVIRONNEMENT CLIENT

Présentation de la planification de la configuration client
Conception et configuration des paramètres système standard
Conception et configuration des paramètres d'Internet Explorer
Conception et configuration des paramètres de sécurité
Conception et implémentation d'une stratégie de groupe
Résolution des problèmes de stratégie de groupe

PLANIFICATION ET DÉPLOIEMENT DES APPLICATIONS ET DES MISES À JOUR DANS LES CLIENTS WINDOWS

Choix de la méthode de déploiement des applications
Déploiement du système Microsoft Office
Planification et configuration des mises à jour des postes de travail à l'aide de l'outil WSUS

PLANIFICATION ET DÉPLOIEMENT DE WINDOWS À L'AIDE DE L'INSTALLATION LTI

Déploiement de Windows - Scénario complexe

Frame IP Formation

Tallen Si Formation

SYS 504

GÉRER LES SERVICES ACTIVE DIRECTORY

OBJECTIFS

- Connaître les solutions disponibles pour la gestion de l'identité et savoir mettre en oeuvre la solution appropriée
- Savoir décrire les composants réseaux fondamentaux et la terminologie et ainsi pouvoir sélectionner les éléments appropriés au travers d'un scénario particulier
- Comprendre comment paramétrer efficacement les GPOs
- Être en mesure d'assurer la sécurité des différents services proposés

PUBLIC

Tout public

2 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

VUE D'ENSEMBLE DE LA PROTECTION DES ACCÈS ET DE L'INFORMATION

Présentation des solutions de protection des accès et de l'information
Vue d'ensemble des solutions de protection des accès et des informations
Vue d'ensemble de Forefront Identity Manager

DÉPLOIEMENT ET ADMINISTRATION AVANCÉS DE AD DS

Déployer AD DS
Déployer et cloner les contrôleurs de domaine virtuels
Déployer les contrôleurs de domaines dans Windows Azure
Administrer AD DS

SÉCURISATION DES SERVICES DE DOMAINE ACTIVE DIRECTORY

Sécuriser les contrôleurs de domaine
Mettre en oeuvre les stratégies de mot de passe et de verrouillage des comptes
Audit des authentifications

SURVEILLANCE, GESTION ET RÉCUPÉRATION DE AD DS

Surveiller AD DS
Gérer la base de données AD DS
Sauvegarde et restauration AD DS et des autres solutions de gestion des identités et des accès

MISE EN OEUVRE ET ADMINISTRATION DES SITES AD DS ET LA RÉPLICATION

Vue d'ensemble de la réplication AD DS
Configurer les sites AD DS
Configurer et surveiller la réplication AD DS

MISE EN OEUVRE DES STRATÉGIES DE GROUPE

Présentation des stratégies de groupe
Mettre en oeuvre et administrer les GPOs
Etendre les stratégies et process des stratégies de groupe
Dépanner les problèmes liés à l'utilisation des GPOs

GESTION DES PARAMÈTRES UTILISATEURS AVEC LES STRATÉGIES DE GROUPE

Mettre en oeuvre les modèles d'administration
Configurer la redirection des dossiers et les scripts
Configurer les préférences des stratégies de groupe

MISE EN OEUVRE DES ACCÈS AUX FICHIERS PARTAGÉS SÉCURISÉS

Vue d'ensemble de DAC
Mettre en oeuvre les composants DAC
Mettre en oeuvre DAC pour le contrôle d'accès
Mettre en oeuvre l'assistance pour les accès refusés
Mettre en oeuvre et gérer les dossiers de travail
Mettre en oeuvre la jonction au lieu de travail (Workplace Join)

DÉPLOIEMENT ET GESTION DES SERVICES DE CERTIFICAT ACTIVE DIRECTORY

Déployer et administrer CAs
Dépanner, maintenir et surveiller CAs

MISE EN OEUVRE ET ADMINISTRATION DE AD RMS

Vue d'ensemble
Déployer et gérer l'infrastructure AD RMS
Configurer la protection du contenu AD RMS
Configurer l'accès externe à AD RMS

MISE EN OEUVRE ET ADMINISTRATION DE AD FS

Vue d'ensemble
Déployer AD FS
Mettre en oeuvre AD FS pour une organisation simple
Déployer AD FS dans un environnement B to B
Etendre AD FS aux clients externes

MISE EN OEUVRE DE WINDOWS AZURE ACTIVE DIRECTORY

Vue d'ensemble
Administrer Windows Azure Active Directory

MISE EN OEUVRE ET ADMINISTRATION DE AD LDS

Vue d'ensemble
Déployer AD LDS
Configurer les instances AD LDS et les partitions
Configurer la réplication AD LDS

SYS 505

ADMINISTRER WINDOWS SERVER

OBJECTIFS

- Être en mesure d'assurer les tâches d'administration courante de Windows Server telles que la gestion des utilisateurs et des groupe ou l'accès réseau
- Savoir planifier le déploiement initial des services Windows Server
- Comprendre comment utiliser efficacement les stratégies de groupe
- Découvrir comment déployer Windows Server par application d'images

PUBLIC

- Administrateurs système chargés de l'administration et de la maintenance des serveurs
- Candidats à la certification Microsoft Certified Solutions Associate (MCSA)

PRÉREQUIS

Professionnels de l'informatique disposant d'une première expérience de l'administration de systèmes informatiques

5 JOURS

POINTS CLÉS DU PROGRAMME

DÉPLOIEMENT ET MAINTENANCE DES IMAGES DE SERVEUR

- Vue d'ensemble des services de déploiement Windows
- Implémentation d'un déploiement avec les services de déploiement Windows
- Administration des services de déploiement Windows

CONFIGURATION ET DÉPANNAGE DU SYSTÈME DNS

- Installation du rôle de serveur DNS
- Configuration du rôle de serveur DNS
- Configuration des zones DNS
- Configuration des transferts de zones DNS
- Gestion et dépannage du système DNS

GESTION DES SERVICES DE DOMAINE ACTIVE DIRECTORY

- Vue d'ensemble d'AD DS
- Implémentation des contrôleurs de domaine virtualisés
- Implémentation de la réplication RODC
- Administration d'AD DS
- Gestion de la base de données AD DS

GESTION DES COMPTES D'UTILISATEURS ET DE SERVICE

- Automatisation de la gestion des comptes d'utilisateurs
- Configuration des paramètres de stratégie de mot de passe et de verrouillage de compte d'utilisateur
- Configuration des comptes de services gérés

IMPLÉMENTATION D'UNE INFRASTRUCTURE DE STRATÉGIE DE GROUPE

- Présentation de la stratégie de groupe
- Implémentation et administration des objets de stratégie de groupe (GPO)
- Étendue et traitement de la stratégie de groupe
- Dépannage de l'application des objets de stratégie de groupe

GESTION DES BUREAUX DES UTILISATEURS AVEC LA STRATÉGIE DE GROUPE

- Implémentation des modèles d'administration
- Configuration de la redirection de dossiers et des scripts
- Configuration des préférences de stratégies de groupe
- Gestion des logiciels à l'aide de la stratégie de groupe

CONFIGURATION ET RÉSOLUTION DES PROBLÈMES D'ACCÈS À DISTANCE

- Configuration de l'accès réseau
- Configuration de l'accès à un réseau privé virtuel (VPN)
- Vue d'ensemble des stratégies réseaux
- Dépannage du service de routage et d'accès à distance
- Configuration de DirectAccess

INSTALLATION, CONFIGURATION ET DÉPANNAGE DU RÔLE DE SERVEURS NPS (NETWORK POLICY SERVER)

- Installation et configuration d'un NPS
- Configuration des clients et serveurs RADIUS (Remote Authentication Dial-In User Service)
- Méthodes d'authentification NPS
- Analyse et dépannage d'un NPS

IMPLÉMENTATION DE LA PROTECTION D'ACCÈS RÉSEAU

- Vue d'ensemble de la protection d'accès réseau
- Vue d'ensemble des processus de contraintes de mise en conformité NAP
- Configuration de la protection d'accès réseau
- Analyse et dépannage de la protection d'accès réseau

OPTIMISATION DES SERVICES DE FICHIERS

- Vue d'ensemble de FSRM (File Server Resource Manager)
- Utilisation de FSRM pour gérer les quotas, les filtres de fichiers et les rapports de stockage
- Implémentation des tâches de classification et de gestion de fichiers
- Vue d'ensemble du système de fichiers distribués (DFS, Distributed File System)
- Configuration des espaces de noms DFS
- Configuration et dépannage de la réplication du système de fichiers distribués (DFS-R)

CONFIGURATION DU CHIFFREMENT ET DE L'AUDIT AVANCÉ

- Chiffrement des fichiers à l'aide du système EFS (Encrypting File System)
- Configuration de l'audit avancé

IMPLÉMENTATION DE LA GESTION DES MISES À JOUR

- Vue d'ensemble de WSUS (Windows Server Update Services)
- Déploiement des mises à jour avec WSUS

ANALYSE DE WINDOWS SERVER

- Outils d'analyse
- Utilisation de l'outil d'analyse des performances
- Analyse des journaux d'événements

SYS 506

MAÎTRISER REMOTE DESKTOP SERVICE ET TSE

OBJECTIFS

- Savoir installer, configurer, gérer un serveur Terminal Services
- Être en mesure de dépanner des serveurs de terminaux sous Windows Server
- Apprendre à garantir l'accès aux applications centralisées à travers une passerelle Web
- Savoir comment simplifier la mobilité, le télétravail et les partenariats
- Rendre plus simple, du point de vue de l'utilisateur, l'intégration des applications virtualisées

PUBLIC

Administrateurs Système Windows

PRÉREQUIS

Bonnes connaissances des systèmes Windows Server et des protocoles réseau TCP/IP

5 JOURS

POINTS CLÉS DU PROGRAMME

REMOTE DESKTOP SERVICES

Gestion courante des connexions
Surveillance du serveur TS
Configurer WSRM pour TS

SERVEURS RDS MULTIPLES

Mise en oeuvre d'une ferme de serveurs RDS
Surveillance de l'environnement RDS

SÉCURISATION DE L'ACCÈS AUX APPLICATIONS RDS À TRAVERS INTERNET AVEC REMOTE DESKTOP GATEWAY

Notions de base
Installation et maintenance

SYS 507

ADMINISTRER DES SERVEURS LINUX

OBJECTIFS

- Acquérir un niveau d'expertise plus élevé sur Linux
- Savoir tirer parti simplement de la richesse modulaire de Linux et du monde Open Source
- Comprendre comment organiser et gérer l'espace disque de gros serveurs Linux
- Apprendre à paramétrer finement le système
- Savoir déployer Linux et l'intégrer avec les autres environnements existants

PUBLIC

Administrateurs système ou réseaux, développeurs souhaitant acquérir confort et autonomie sur Linux

5 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

ADMINISTRER LES SERVEURS DE FAÇON PROFESSIONNELLE

La philosophie de l'administration Linux
Les outils de l'expert : logger, la commande script, crontab, sudo, RCS
Où trouver de l'aide (mailing-list, forums, ...) ?

LES SYSTÈMES DE FICHIERS JOURNALISÉS, LES SYSTÈMES DE FICHIERS SPÉCIAUX

Comparaison des systèmes de fichiers journalisés (ext3, reiserfs, xfs, jfs)
Étude du système ext3 (RedHat)
Étude du système reiserfs (SUSE)
Les systèmes de fichiers spéciaux (tmpfs, unionfs)

PARAMÉTRAGE AVANCÉ DES SYSTÈMES DE FICHIERS ET DES DISQUES

Les quotas
Panorama des techniques RAID, le raid logiciel
Mettre en oeuvre des ACL, des attributs Linux
La gestion de l'espace de swap

LA GESTION DES VOLUMES LOGIQUES (LVM)

Les concepts et les commandes de base du LVM
Les pratiques avancées : Sauvegarde, Stripping, Snapshots...

MODIFIER LE NOYAU

Pourquoi recompiler le noyau ?
Patcher et compiler le noyau
Ajouter un module et modifier les paramètres du noyau sans recompiler

LA GESTION DES PÉRIPHÉRIQUES

Comment sont gérés les périphériques sous Linux, les commandes d'informations ?
L'ajout d'un périphérique
L'étude de quelques périphériques (disques, cdrom, lecture de cartouche, ...)

LE DÉMARRAGE D'UN SYSTÈME LINUX

Les chargeurs lilo et Grub
Paramétrer de manière souple le démarrage avec les fichiers initrd
Utiliser un système bootable de dépannage (Knoppix...)
Fabriquer un CD/clé bootable

GARANTIR L'INTÉGRITÉ DES DONNÉES : LES SAUVEGARDES

Mettre en oeuvre les sauvegardes incrémentales
Fabriquer une sauvegarde réseau
Faire une sauvegarde barre-métal : les logiciels libres existants (Mondo...)

AMÉLIORER LES PERFORMANCES DU SYSTÈME

Créer des classes d'imprimantes
Améliorer les performances : hdparm, ulimit, les paramètres de/proc, tmpfs, ...

LE DÉPANNAGE

Une approche méthodique du dépannage
Les outils de l'expert : strace, lsof, ...
Se prémunir des problèmes

COMPLÉMENTS SUR L'AUTOMATISATION DES TÂCHES

Le service anacron
La rotation des journaux de bord

SYS 508

MAÎTRISER L'ENVIRONNEMENT CITRIX

OBJECTIFS

- Savoir installer Citrix XenApp pour Windows Server et les clients associés
- Apprendre à utiliser les consoles et les outils d'administration pour gérer les ressources, les stratégies et les paramètres d'une ferme de serveurs
- Savoir installer, configurer et déployer XenApp
- Maîtriser les consoles d'administration
- Apprendre à gérer le déploiement et la variété des plug-ins
- Savoir mettre en oeuvre les interfaces Web et le streaming d'applications

PUBLIC

Administrateurs XenApp Server. Toute personne en charge de déployer une solution «client léger» basée sur la technologie Citrix. Les ingénieurs systèmes, architectes réseaux et consultants sont aussi des candidats appropriés pour cette formation

PRÉREQUIS

Une bonne connaissance de l'environnement Windows Server
Connaissance des serveurs SQL ou des serveurs de bases de données

5 JOURS

POINTS CLÉS DU PROGRAMME

INTRODUCTION À XENAPP
- Les différentes éditions
- Les fonctionnalités
- L'architecture
- Console Delivery Services

GESTION DES LICENCES
- Le système de licences XenApp
- Console d'administration des licences
- Installation du serveur de licences
- Fichiers de licences
- Haute disponibilité

INSTALLATION DE XENAPP
- Décisions à prendre avant l'installation
- XenApp Server Role Manager
- Modalités d'installation de l'interface Web
- Installation et configuration automatisées
- Pré-requis matériels
- Pré-requis logiciels
- Options de configuration

CONFIGURATION DE L'ADMINISTRATION
- Délégation de l'administration
- Audit des changements de configuration

INSTALLATION ET CONFIGURATION DE L'INTERFACE WEB
- Architecture et communication
- Installation
- Création d'un site
- Configuration du site
- Dépannage

PUBLICATION D'APPLICATIONS ET DE CONTENU
- Publication de ressources
- Applications hébergées dans des machines virtuelles
- Présentation des ressources publiées aux utilisateurs
- Paramètres de publication avancés
- Configuration des ressources publiées
- Résolution des problèmes de livraison des applications

APPLICATIONS LIVRÉES EN STREAMING
- Architecture
- Client en mode déconnecté
- Citrix Streaming Profiler
- Méthode de livraison des applications
- Dépannage

STRATÉGIES
- Intégration avec la stratégie de groupes Windows
- Évaluation des stratégies
- Règles de stratégie
- Filtrage des stratégies
- Modélisation et dépannage des stratégies

RÉPARTITION DE LA CHARGE
- Gestionnaire de la charge
- Équilibrage de la charge
- Calcul de la charge
- Configuration des évaluateurs de charge
- Stratégies d'équilibrage de charge
- Équilibrage de charge préférentiel
- Résolution des problèmes d'équilibrage de charge

OPTIMISATION DE L'EXPÉRIENCE UTILISATEUR
- Optimisation des performances pour les sessions
- Profils utilisateurs
- Résolution des problèmes

APPLICATIONS EN LIBRE-SERVICE
- Citrix Receiver
- Citrix Merchandising Server
- Citrix Dazzle
- Plug-ins
- Dépannage

IMPRESSIONS
- Concepts de base
- Comportement par défaut
- Provisionnement des imprimantes
- Routage des impressions
- Pilotes d'imprimante
- Gestionnaire d'impression universel Citrix
- Imprimantes réseau attribuées par l'administrateur
- Contrôle de l'espace de travail et imprimantes de proximité
- Préférences d'impression
- Gestion de la bande passante
- Dépannage des problèmes d'impression

SÉCURITÉ DE XENAPP
- Solutions de sécurité XenApp
- SecureICA
- Relais SSL
- Acces Gateway
- Configuration de l'interface Web
- Bonnes pratiques
- Résolution des problèmes

SURVEILLANCE
- Surveillance et récupération automatiques
- Supervision EdgeSight
- Contrôle de l'utilisation des licences
- Workflow Studio
- Accès à la ferme de serveurs à partir de PowerShell
- Administration en ligne de commande

COMPOSANTS ADDITIONNELS
- SmartAuditor
- Citrix Single Sign-On (ex Password Manager)
- EasyCall Voice Services
- Citrix Branch Optimization
- Provisioning Services
- Power and Capacity Management
- XenServer

SYS 509

ADMINISTRER MICROSOFT OFFICE 365

OBJECTIFS

- Comprendre les différentes offres de services
- Être en mesure d'installer les services et outils
- Comprendre comment gérer les utilisateurs
- Être en mesure de paramétrer et personnaliser les différents outils en ligne, de Lync à SharePoint

PUBLIC

Administrateurs système et réseau

5 JOURS

OUTILS PÉDAGOGIQUES

- Diffusion du cours
- Études de cas
- Travaux pratiques

POINTS CLÉS DU PROGRAMME

1ÈRE PARTIE : GÉNÉRALITÉS, DÉCOUVERTE

Présentation générale
Les offres Office 365
Présentation des applications Office Web Apps
Les services dédiés au partage

INSTALLATION DES SERVICES ET OUTILS

Vérifier les mises à jour du système
Installer et configurer les services et outils

ESPACE DE TRAVAIL

Description de la page d'accueil Administrateur
Modifier son profil

2ÈME PARTIE : GESTION DES UTILISATEURS

CRÉATION ET MODIFICATION

Les types de comptes
Créer un compte utilisateur
Ajouter plusieurs utilisateurs
Modifier un compte utilisateur
Modifier les paramètres courrier d'un utilisateur
Modifier plusieurs comptes
Supprimer un utilisateur
Réinitialiser un mot de passe

GÉRER LA LISTE DES UTILISATEURS

Afficher la liste des utilisateurs
Rechercher des utilisateurs
Trier la liste des utilisateurs
Filtrer la liste des utilisateurs
Créer une vue d'utilisateur

3ÈME PARTIE : ADMINISTRATION DES SERVICES

LYNC ONLINE

Accéder au panneau de configuration
Configurer la fédération de domaine
Activer/désactiver la messagerie instantanée publique
Gérer les droits des utilisateurs

EXCHANGE ONLINE

Accéder au panneau de configuration
Créer une boîte aux lettres d'utilisateur
Nouvelle boîte aux lettres de salle
Importer un fichier CSV
Trier la liste des boîtes aux lettres
Filtrer la liste des boîtes aux lettres
Rechercher une boîte aux lettres
Modifier les paramètres d'une boîte aux lettres
Supprimer des boîtes aux lettres
Restaurer une boîtes aux lettres supprimée
Réinitialiser le mot de passe
Attribuer une licence aux utilisateurs de boîte aux lettres
Créer un groupe de distribution
Modifier les propriétés d'un groupe de distribution

4ÈME PARTIE : SHAREPOINT ADMINISTRATION

GÉNÉRALITÉS

Accéder à la page des paramètres du site d'équipe
Accéder aux paramètres d'un autre site
Les objets d'un site
Afficher la page d'accueil d'un site - méthode 1
Afficher la page d'accueil d'un site - méthode 2
Afficher tout le contenu d'un site
Naviguer dans l'arborescence d'un site

GESTION D'UN SITE

Créer un nouveau site rapide
Créer un site
Personnaliser le volet Lancement rapide
Personnaliser la barre de liens supérieure
Modifier le thème d'un site
Modifier le nom, le logo et l'adresse d'un site
Ajouter/modifier le propriétaire du site principal
Supprimer un site - Méthode 1
Supprimer un site - Méthode 2
Restaurer un site supprimé

NIVEAUX D'AUTORISATION

Les différents niveaux d'autorisation
Afficher les niveaux d'autorisation
Créer un niveau d'autorisation
Modifier un niveau d'autorisation
Supprimer un niveau d'autorisation
Annuler l'héritage du site parent

GROUPES D'UTILISATEURS

Afficher les groupes d'utilisateurs
Créer un groupe d'utilisateurs
Ajouter un utilisateur à un groupe
Modifier un groupe d'utilisateurs
Attribuer des niveaux d'autorisation à un utilisateur/groupe
Modifier les niveaux d'autorisation d'un groupe

5ème partie : Pages SharePoint

CRÉATION

Accéder à votre site d'équipe
Créer une nouvelle page
Afficher la liste des pages d'un site
Afficher une page en mode Édition
Choisir la disposition d'une page
Saisie et mise en valeur du texte
Enregistrer les modifications d'une page

GESTION

Définir la page en tant que page d'accueil
Renommer une page
Supprimer une ou plusieurs pages
Restaurer une page supprimée
Envoyer le lien d'une page par messagerie électronique

GESTION DU SITE

Optimiser la visibilité de votre site
Partager le site Web

SYS 510

ADMINISTRER SYSTEM CENTER

OBJECTIFS

- Comprendre comment planifier et assurer le déploiement de la solution
- Savoir délivrer des applications virtuelles et en contrôler l'accès
- Disposer des connaissances nécessaires à la constitution d'un catalogue de services privés
- Être en mesure de surveiller et protéger l'infrastructure avec Operations Manager et Data Protection Manager

PUBLIC

Administrateurs de Datacenter en charge de la conception de Clouds privés

PRÉREQUIS

- Disposer d'une solide expérience de Windows Server , d'Active Directory et des réseaux
- La connaissance d'Hyper-V, des précédentes versions de System Center et de SharePoint est un plus pour suivre cette formation

5 JOURS

POINTS CLÉS DU PROGRAMME

PLANIFICATION

- Le concept de Cloud privé
- Pré-requis pour le déploiement
- Définition des composants
- Déploiement de l'infrastructure avec System Center
- Déploiement de clusters Hyper-V avec Virtual Machine Manager (VMM)

CONFIGURATION ET DÉPLOIEMENT DE L'INFRASTRUCTURE

- Architecture et composants de Virtual Machine Manager
- Installation et mise à niveau de Virtual Machine Manager
- Configuration de la sécurité et des rôles utilisateurs dans VMM

MAINTENANCE ET EXTENSION DE L'INFRASTRUCTURE

- Serveur PXE et serveur de mise à jour
- Déploiement automatisé de serveurs Hyper-V
- Configuration du rôle de serveur de mises à jour
- Création et déploiement d'un jeu de mises à jour minimum

LIVRAISON D'APPLICATIONS VIRTUELLES

- Déploiement dynamique des applications
- Packages de déploiement We Server App-V
- Séquencement et déploiement des applications virtuelles

CRÉATION DES BRIQUES DE BASE DU CLOUD

- Profils de systèmes d'exploitation hébergés
- Profils matériels
- Déploiement de SQL Server au moyen de profils SQL Server
- Profils applicatifs
- Modèles de machines virtuelles
- Utilisateurs du portail libre-service

DÉPLOIEMENT ET CONFIGURATION DES ACCÈS DU PREMIER CLOUD

- Introduction
- Installation et configuration d'Application Controller
- Création et gestion des services et des modèles de service

SURVEILLANCE DE L'INFRASTRUCTURE AVEC OPERATIONS MANAGER

- Architecture et sécurité
- Mise à niveau
- Notifications
- Management Packs
- Intégration avec System Center

EXTENSION ET PERSONNALISATION DES FONCTIONNALITÉS DE SURVEILLANCE

- Portail SharePoint
- Modèles de surveillance
- Surveillance des applications distribuées

GESTION DU SERVICE AVEC SERVICE MANAGER

- Architecture
- Mise à niveau
- Éléments de travail
- Connecteurs
- Notifications
- Gestion des incidents et des problèmes

CONSTITUTION D'UN CATALOGUE DE SERVICES PRIVÉ

- Définition
- Cloud Service Process Management Pack
- Prise en charge des demandes de service
- Configuration des offres de service
- Gestion du niveau de service

PROTECTION DE L'INFRASTRUCTURE AVEC DATA PROTECTION MANAGER

- Architecture et sécurité
- Mise à niveau
- Protection globale du Cloud
- Protection des applications
- Restauration des applications

AUTOMATISATION ET STANDARDISATION DU CLOUD

- Présentation de System Center Orchestrator
- Déploiement et configuration des composants de base
- Configuration des packs d'intégration
- Création de Runbooks
- Exécution d'un Runbook à partir de Service Manager

Frame IP Formation

Tallen SI Formation

SYS 511

METTRE EN OEUVRE ET GÉRER LES FONCTIONNALITÉS AVANCÉES D'EXCHANGE SERVER

OBJECTIFS

- Être en mesure d'installer et déployer Exchange Server
- Apprendre à configurer la sécurité du système de messagerie Exchange Server
- Savoir planifier et mettre en oeuvre les sauvegardes et restaurations
- Être en mesure d'implémenter une messagerie unifiée dans Exchange Server

PUBLIC

Administrateurs de Microsoft Exchange Server 2003 ou Exhange Server 2007

PRÉREQUIS

- Connaissances de l'administration de Windows Server et Active Directory Services Domain Services (AD DS)
- Avoir une expérience dans l'administration d'Exchange Server 2003 ou 2007 est un plus

5 JOURS

POINTS CLÉS DU PROGRAMME

DÉPLOIEMENT DE MICROSOFT EXCHANGE SERVER

Vue d'ensemble de la configuration requise pour Exchange Server
Installation des rôles serveur Exchange Server
Exécution d'une installation d'Exchange Server

CONFIGURATION DES SERVEURS DE BOÎTES AUX LETTRES

Vue d'ensemble des outils d'administration Exchange Server
Configuration des serveurs de boîtes aux lettres
Configuration des dossiers publics

GESTION D'OBJETS DESTINATAIRES

Gestion des boîtes aux lettres
Gestion d'autres destinataires
Configuration de stratégies d'adresse de messagerie
Configuration de listes d'adresses
Exécution des tâches de gestion des destinataires en bloc

GESTION DE L'ACCÈS CLIENT

Configuration du serveur d'accès au client
Configuration des services d'accès au client pour des clients Outlook
Configuration d'Outlook Web App
Configuration de la messagerie mobile

GESTION DU TRANSPORT DE MESSAGES

Vue d'ensemble du transport de messages
Configuration du transport de messages

IMPLÉMENTATION DE LA SÉCURITÉ DE LA MESSAGERIE

Déploiement des serveurs de transport Edge
Déploiement d'une solution antivirus
Configuration d'une solution anti-spam
Configuration de la messagerie SMTP sécurisée

IMPLÉMENTATION DE LA HAUTE DISPONIBILITÉ

Vue d'ensemble des options de haute disponibilité
Configuration de base de données de boîtes aux lettres hautement disponibles
Déploiement de serveurs autres que des serveurs de boîtes aux lettres hautement disponibles

IMPLÉMENTATION DE LA SAUVEGARDE ET DE LA RÉCUPÉRATION

Planification de la sauvegarde et de la récupération
Sauvegarde d'Exchange Server
Restauration d'Exchange Server

CONFIGURATION DE LA STRATÉGIE ET DE LA CONFORMITÉ DE LA MESSAGERIE

Présentation de la stratégie et de la conformité de la messagerie
Configuration des règles de transport
Configuration de la journalisation et de la recherche dans plusieurs boîtes aux lettres
Configuration de la gestion des enregistrements de messagerie
Configuration des archives personnelles

SÉCURISATION DE MICROSOFT EXCHANGE SERVER

Configuration du contrôle d'accès basé sur les rôles
Configuration de la sécurité pour les rôles serveur dans Exchange Server
Configuration de l'accès Internet sécurisé
Maintenance de Microsoft Exchange Server
Analyse d'Exchange Server
Maintenance d'Exchange Server
Résolution des problèmes liés à Exchange Server

MISE À NIVEAU D'EXCHANGE SERVER

Vue d'ensemble de la mise à niveau vers Exchange Server

IMPLÉMENTATION DE LA MESSAGERIE UNIFIÉE

Vue d'ensemble de la téléphonie
Introduction à la messagerie unifiée
Configuration de la messagerie unifiée

FONCTIONNALITÉS AVANCÉES DANS EXCHANGE SERVER

Déploiement de solutions hautement disponibles pour plusieurs sites
Implémentation du partage fédéré

SYS 512

VIRTUALISATION AVEC MICROSOFT HYPER-V

OBJECTIFS

- Apprendre à installer l'hyperviseur Hyper-V
- Découvrir les nouvelles fonctionnalités de Hyper-V sous Windows Server
- Être capable d'optimiser la configuration de l'hyperviseur et des machines virtuelles pour la montée en charge et la disponibilité des services

PUBLIC

Toute personne en charge de la conception ou de la mise en oeuvre d'un environnement virtualisé sous Windows Server

PRÉREQUIS

- Bonnes connaissances de Windows Server
- Bonnes connaissances des réseaux TCP/IP

5 JOURS

POINTS CLÉS DU PROGRAMME

PRÉPARATION

Généralités sur les outils de virtualisation Microsoft
Évaluation des systèmes en vue de leur virtualisation
Mise en place du projet

MISE EN OEUVRE DE LA VIRTUALISATION DE SERVEUR AVEC HYPER-V

Installation du rôle de serveur Hyper-V
Définition de la configuration des commutateurs virtuels
Configuration des réseaux virtuels

DISQUES ET MACHINES VIRTUELS

Création et configuration de disques virtuels
Création et configuration de machines virtuelles
Paramétrage des machines virtuelles
Captures instantanées
Importation de machines virtuelles

HYPER-V ET LES RÉSEAUX

Fonctionnalités avancées des interfaces réseaux virtuelles
Virtualisation de réseaux
Commutateur virtuel extensible

MONTÉE EN CHARGE

Options disponibles sous Windows Server
Non-Uniform Memory Access (NUMA)
Comparaison avec les versions précédentes

HYPER-V REPLICA ET SOLUTIONS DE REPRISE SUR INCIDENT

Généralités
Configuration de Hyper-V Replica
Basculement sur un site de secours
Sauvegardes

MOBILITÉ DES MACHINES VIRTUELLES

Live Migration - Généralités
Storage Migration
Live Migration - Sécurité
Live Migration avec SMB

SYS 513

VIRTUALISATION DU POSTE DE TRAVAIL VID

OBJECTIFS

- Connaître les technologies de virtualisation du poste de travail
- Être en mesure de sélectionner la solution plus adaptée à son contexte
- Apprendre à configurer et à distribuer des applications virtualisées à destination des utilisateurs
- Savoir créer, configurer et distribuer des machines virtuelles à destination des utilisateurs
- Être en mesure de mettre en oeuvre une infrastructure de postes de travail virtuels

PUBLIC

Architectes, ingénieurs et administrateurs système ayant en charge la mise en place de postes de travail virtualisés au sein de leur entreprise

PRÉREQUIS

- Bonnes connaissances des systèmes d'exploitation Windows
- Notions de base de la virtualisation de systèmes

5 JOURS

POINTS CLÉS DU PROGRAMME

VUE D'ENSEMBLE DES SCÉNARIOS DE VIRTUALISATION DE BUREAU

Vue d'ensemble de la virtualisation
Vue d'ensemble de la gestion de la virtualisation
Planification d'un déploiement de virtualisation de bureau et d'applications

CONFIGURATION DES SERVICES BUREAU À DISTANCE ET DE REMOTEAPP

Vue d'ensemble des services Bureau à distance
Publication de RemoteApp à l'aide des services Bureau à distance
Accès aux programmes RemoteApp à partir de clients

IMPLÉMENTATION DE LA VIRTUALISATION DE L'ÉTAT UTILISATEUR

Vue d'ensemble de l'état utilisateur
Configuration des profils itinérants et de la redirection de dossiers

CONFIGURATION DE L'INFRASTRUCTURE VDI (VIRTUAL DESKTOP INFRASTRUCTURE)

Vue d'ensemble de Windows Server Hyper-V
Présentation de VDI
Configuration des bureaux virtuels personnels et regroupés
Utilisation de la console Application Virtualization Management Console
Publication d'applications dans l'environnement App-V
Exécution de tâches d'administration avancées pour la virtualisation d'applications

SÉQUENCEMENT DES APPLICATIONS POUR LA VIRTUALISATION

Vue d'ensemble du séquencement des applications
Planification et configuration de l'environnement du séquenceur
Exécution du séquencement des applications
Scénarios de mise en séquences avancés

RÉSUMÉ DES TECHNOLOGIES DE VIRTUALISATION DE BUREAU

Étude des technologies de virtualisation de bureau
Scénarios d'utilisation réels

Frame iP Formation

SYS 514

VIRTUALISATION AVEC VMWARE, VSPHERE

OBJECTIFS

A l'issue de la formation les participants devront savoir installer et configurer ESX, vCenter Server, configurer et gérer le stockage et la mise en réseau avec vCenter Server, déployer et gérer les machines virtuelles, les accès utilisateurs à l'infrastructure virtuelle VMware, savoir optimiser l'évolutivité, gérer l'utilisation des ressources, la protection de données avec vCenter Server et appliquer les mises à jour avec vCenter Update Manager et gérer la haute disponibilité.

PUBLIC

Admin système en charge de VMware ESX / ESXi et vCenter.

PRÉREQUIS

Expérience en administration de systèmes Microsoft et Linux

3 JOURS

POINTS CLÉS DU PROGRAMME

INTRODUCTION À LA VIRTUALISATION VMWARE

La virtualisation, les composants vSphere

CONFIGURATION ESXI/ESX

INSTALLATION ET UTILISATION DE VCENTER SERVER

Installation de vCenter Server et utilisation du client vSPhere pour gérer la hiérarchie des objets de l'infrastructure virtuelle

MISE EN RÉSEAU

Configuration de vNetwork, des Switches virtuels standards, des Distributed Switches, des ports et connexions réseau

STOCKAGE

Technologies de gestion du stockage

MACHINES VIRTUELLES

Déploiement de machines virtuelles avec utilisation de modèles, VMware vCenter Converter, Guided Consolidation.

Modification, gestion et migration de machines virtuelles

CONTRÔLE D'ACCÈS

Contrôle des accès au travers des rôles et permissions

SURVEILLANCE DES RESSOURCES

Audit de charge et surveillance avec vCenter Server

ÉVOLUTIVITÉ

Migration avec VMware vMotion™

Mise en place de pools de ressources et d'un cluster DRS (VMware Distributed Resource Scheduler)

HAUTE DISPONIBILITÉ ET PROTECTION DE DONNÉES

Mise en place d'un cluster HA (High Availability)

Sauvegarde et restauration de machines virtuelles avec vCenter Data Recovery

GESTION DE LA CONFIGURATION

Application et installation de mises à jour avec vCenter Update Manager

INSTALLER ESX

Installation de VMware ESX

UNE COUVERTURE NATIONALE

FrameIP et TallenSI disposent d'une couverture nationale avec une gamme complète de solutions pour vos formations! Dans nos centres de formation, que ce soit sur La Défense, Paris, Rouen, Lille ou Caen, chaque salle de cours offre :

- Des équipements informatiques, réseaux et internet performants
- Un environnement de travail agréable et idéal pour la concentration nécessaire de nos participants
- Un espace suffisant pour permettre au formateur d'organiser sa formation en ateliers, jeux de rôle, travaux pratiques, etc.
- Un matériel pédagogique de pointe

Tous nos centres ont le sens du service. Ils disposent d'un accueil, d'un espace pause avec café et viennoiseries, possibilité de déjeuner aux alentours du centre.

FrameIP et TallenSI disposent de 10 salles de formations de dimensions suffisantes pour accueillir de 1 à 15 personnes.

Une journée de formation dure 8 heures.

Nos moyens techniques

- FrameIP et TallenSI met à la disposition de chaque participant un ordinateur portable équipé des logiciels de formation.
- Un support de cours pour chaque stagiaire.
- Toutes nos salles sont équipées d'un vidéoprojecteur, d'un tableau blanc et d'un paper board.
- En plus, pour toutes les formations techniques, le formateur apporte tout le matériel nécessaire à la compréhension des formations de type Système, Réseau, Sécurité et Téléphonie sur IP.

Modalités d'inscription

Un serveur « inscription » est disponible sur nos sites internet : ***www.frameip.fr*** ou ***www.tallensi.fr***, uniquement dédiés à votre structure. En effet, avec votre login et mot de passe en tant qu'administrateur, vous avez une visibilité sur l'ensemble des formations mises à disposition de vos utilisateurs, le nombre d'inscriptions, gérer les sessions. Pour vos utilisateurs, une inscription en ligne directement, simple et facile d'utilisation, en remplissant un formulaire.

FRAMEIP PROTÈGE L'ENVIRONNEMENT

Dans le but de réduire leur empreinte carbone, TallenSI et FrameIP ont revu toutes leurs activités et méthodes de travail afin de veiller à ce que les processus aient le minimum d'impact sur l'environnement. Nous avons notamment mis en place une procédure de protection de l'environnement en réduisant considérablement l'utilisation de papier au sein même de l'entreprise, mais également lors des formations en dématérialisant au maximum les supports d'informations matériels.

C'est pourquoi chaque participant reçoit un support de cours électronique via une clé USB pour qu'il puisse, une fois la formation achevée, garder le bénéfice de l'enseignement, en particulier, sur les fondamentaux transmis. L'avantage est de vous offrir le cours sous format électronique intégrant l'ensemble des points clés et éléments techniques de la formation suivie.

FrameIP
formation@frameip.fr
Téléphone : 0 805 280 022
Site : www.frameip.fr

TallenSI
formation@tallensi.fr
Téléphone : 0 805 280 200
Site : www.tallensi.fr