

Le protocole d'authentification Kerberos

Plan de Formation

Module 1 : Introduction

- Qu'est ce que Kerberos
- Avantages de Kerberos
- Les RFC
- Architecture système

Module 2 : le protocole Kerberos

- Composants Kerberos
- Messages Kerberos
- Contenu des tickets Kerberos
- PAC : Construction des jetons (group Membership)
- REALM
- UPN
- SPN
- Ports et paramétrage
- Localisation des KDC
- Synthèse des protocoles de chiffrement et de signature
-

Module 3 : NTLM

- Versions LanManager
- Comparatifs
- Mécanisme d'authentification
- LMCompatibilityLevel
- Chiffrement

Module 4 : Scénarios

- Authentification Intra Domaine
- Authentification Inter domaine
- Authentification d'un utilisateur d'un domaine sur une station de travail d'un autre domaine accédant une ressource d'un troisième domaine.
- Authentification Inter forêt

- Authentification vers un domaine non approuvé
- Fonctionnement en NTLM

Module 5 : Détails supplémentaires

- Ports à ouvrir à travers les firewall
- Etablissement de relations d'approbation
- Objets TDO et mécanismes de changement de mot de passe.
- GPO Inter Forêt
- Sites Inter Forêt
- SID Filtering
- Authentification sélective
- msDS-SPNSuffixes
- Résumé taille du jeton d'accès
-

Module 6 : Authentification par cartes à puce

- Mécanismes
- Préparation de l'environnement
- Paramétrage des comptes

Module 7 : La délégation Kerberos

- Mécanisme
- Pré requis
- Windows 2000 : délégation non contrainte
- Contrainte de délégation
- Transition de protocole : extension S4U

Module 8 : Interopérabilité Unix/Linux

- Implémentation MIT
- Interopérabilité avec Microsoft
- Authentification client MIT dans domaine Windows
- Authentification Windows dans domaine MIT
- Ktpass, ksetup, kinit
-

Module 9 : Diagnostic et résolution de problèmes

- Trace réseau
- Utilitaires klist et kerbtray
- Vérification des SPN
- Journal d'évènement client, serveur, DC
- Augmentation niveau de diagnostic sur les DC

À propos de ce cours

	<p>Cette section décrit brièvement le cours et ses objectifs, le profil des stagiaires ainsi que les connaissances préalables requises.</p>
Description	<p>Ce cours animé par un instructeur et réparti sur trois journées permet aux stagiaires d'acquérir les connaissances et la compréhension des mécanismes d'authentification en environnement Microsoft.</p>
Profil des stagiaires	<p>Cette formation s'adresse à des équipes de chefs de projet ou d'exploitants devant maintenir l'Active Directory et être responsables des services d'authentification.</p>
Connaissances préalables	<p>Pour participer à ce cours, les stagiaires doivent avoir une bonne connaissance des annuaires Active Directory et LDAP.</p>
Objectifs	<p>L'objectif de cette formation est de présenter aux participants tous les concepts de Kerberos et leur transférer les connaissances et compétences nécessaires à l'administration d'un domaine Windows.</p> <p>À la fin de ce cours, les stagiaires seront à même d'effectuer les tâches suivantes :</p> <ul style="list-style-type: none">■ Paramétrer Kerberos et diagnostiquer les problèmes d'authentification au sein d'une forêt et entre forêts distincts.■ Mettre en place un service d'authentification Kerberos en environnement hétérogène (MIT, Linux, Unix).

Calendrier du cours

Voici une estimation horaire du déroulement du cours. Il est possible que vos horaires soient différents de ceux indiqués dans le tableau suivant :

Premier jour

Début	Fin	Module
9:00	10:30	Module 1 Introduction
10:30	10:45	Pause
10:45	12:00	Module 2 : Le protocole Kerberos
12:00	13:00	Déjeuner
13:00	14:30	Module 2 (Suite)
14:30	14:45	Pause
14:45	15:30	Démo et travaux pratiques : Analyse de trace réseau.
15:30	18:00	Module 3 : NTLM

Deuxième jour

Début	Fin	Module
9:00	9:30	Rappels et Contrôle des acquis du premier jour
9:30	10h30	Module 4 :
10:30	10:45	Pause
10:45	12:00	Module 4 : (Suite)
12:00	13:00	Déjeuner
13:00	14:30	Module 4 : (Suite)
14:30	14:45	Pause
14:45	15:30	Démo : Analyse de trace réseau.
15 :30	18 :00	Module 5 : Détails supplémentaires

Troisième jour

Début	Fin	Module
9:00	9:30	Contrôle des acquis du deuxième jour
9:30	10:30	Module 6 : authentification par carte à puce.
10:30	10:45	Pause
10:45	12:00	Module 7 : Délégation Kerberos
12:00	13:00	Déjeuner
13:00	14:30	Module 8 : Interopérabilité Unix
14:30	14:45	Pause
14:45	17:00	Module 9 : Diagnostics et résolution de problèmes.