SSO par Kerberos Constrained Delegation sur APM - Best Practices

Matthieu Dierick, 2015-24-01

Mettre en place un SSO sur APM par Delegation Kerberos n'est pas chose aisée. Voici 5 recommandations ou best practices pour réussir votre SSO par **Kerberos Constrained Delegation**, surtout lorsque l'on souhaite authentifier des utilisateurs venant de **plusieurs domaines**.

1. Le compte de délégation AD pour l'APM **doit être** dans le même domaine que la ressource demandée. Par exemple, si vous avez 2 domaines, ALPHA.COM et BRAVO.COM, et que votre serveur Sharepoint est dans ALPHA.COM, le compte de délégation AD pour APM doit se trouver dans ALPHA.COM. Les utilisateurs quand à eux, peuvent se trouver dans l'un ou l'autre domaine. Ceci est du à un prérequis de la RFC sur le Kerberos Contraines Delegation qui ne permet pas de traverser les domaines.

2. La valeur du Logon Name du compte de délégation (userPrincipalName) **doit être** dans le format d'un servicePrincipalName (SPN), et vous devez utiliser cet SPN dans la configuration du Account Name du SSO. Par exemple, vous avez un compte de délégation nommé « krb.srv » dans le domaine ALPHA.COM. Le Logon Name de l'utilisateur (userPrincipalName) peut être « host/krb.srv.alpha.com ». Le compte de servicePrincipalName doit être aussi « host/krb.srv.alpha.com ». Si vous utiliser un format non-SPN dans le champs Logon Name, ou pour la valeur du Pre-Windows 2000 (sAMAccountName) dans le profile SSO Kerberos, vous aurez une erreur du type « service principal unknown » quand vous essaierez d'authentifier des utilisateurs venant de domaines différents.

3. Les domaines **doivent avoir** une relation d'approbation **bi-directionnelle** (bi-directional transitive trust). L'extension Kerberos Protocol Transition (KPT) l'impose. Vous ne pourrez pas faire de KPT/KCD avec un trust non transitif et/ou une relation uni-directionnel.

4. L'APM doit être capable de joindre chaque KDC de **chaque** domaine sur le port 88 en TCP et en UDP. En deux mots, l'APM doit discuter avec chaque KDC :

    a. A son KDC local pour avoir un ticket pour l'autre KDC

    b. A l'autre KDC pour avoir un ticket pour l'utilisateur

    c. Et finalement à son KDC local pour avoir un ticket pour la ressource applicative.

5. Vous devez injecter le **realm du domaine de l'utilisateur** dans la configuration SSO pour que cela fonctionne. Pour cela, il faut le récupérer. Donc soit l'utilisateur le définit dans la page de login (via une selection box ou directement dans le login name sous le format domain\user), soit vous allez le récupérer via un Query AD/LDAP par exemple. Une fois le domaine connu, vous n'avez plus car remplir la variable session.logon.last.domain → session.logon.last.domain = expr { "BRAVO.COM"}.

Source : Thanks to my colleague Kevin Stewart

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com