Red Hat Identity Management の利用前にチェックするべき項目

レッドハット株式会社

2018-08-15

森若 和雄 <kmoriwak@redhat.com>

このスライドの位置付けと目的

- 対象
  - Red Hat Identity Managementの構築をこれから行う人
- 目的
  - 構築前に考慮するべき点や、避けるべき構成などについての情報提供

概要

- クライアントについて
- IdMサーバについて
- 必要サーバ数
- サーバ構成
- 利用したい機能を決める
- NG集

クライアントについて

- ユーザ数とクライアント数、クライアントOSの確認
  - クライアント側がサポートされるのはRHELの場合のみ
  - IdMは1企業内での利用を想定しており10万ユーザ、5万グループ規模でテストされています。
- SSSDが利用できるOSか?
  - SSSDのバージョンにより利用できる機能がかわるので要確認
- SSSDが利用できないOSを利用するか?
  - LDAP、Kerberosで接続できるがあまりスケールしないので要注意

必要サーバ数について

- 最低2システムは必要
  - IdMが壊れると全システムに影響するため可用性対策として必要
  - ネットワーク的にとても近い場合をのぞけば
    2 × (データセンタ数) あるとよい
- マルチマスタレプリケーションによるActive-Active構成が基本
  - 1サーバあたり目安としてはクライアント2000〜3000台程度
  - サポート上限は60台マルチマスタ構成

サーバ構成について

- 物理サーバ・仮想サーバのどちらでもよい
- メモリ量の目安
  - 10,000ユーザ 100グループ: 最低3GB RAMと1 GB swap
  - 100,000ユーザ 50,000グループ: 最低16 GB RAMと4 GB swap
- 必須: IPv6が有効、FQDNのホスト名、DNSの正引き逆引きが可能であること
- 推奨: RHEL 7の最新版で構築、SELinuxをenforcing

※ コンテナ対応は現在のところtechnology preview

利用したい機能を決める(1/3)

- DNS
  - IdMの自動検出・自動冗長化・負荷分散、ドメイン参加による自動登録に利用
  - 外部のDNSを利用するか、IdM内蔵DNSだけを使う場合にはroot zoneをもたせるかどうか
- OTP
  - IdM内蔵のHOTP/TOTPを利用するか、サードパーティOTPソリューションをRADIUSで統合するか
- スマートカード認証
  - ドキュメントに動作確認済みスマートカード一覧があるので確認する

利用したい機能を決める(2/3)

- CA局
  - サービスとユーザ用のみ発行可能
  - 自己署名か、外部CA局から発行された証明書を利用するか?
  - CA局を構築する場合は必ず2つ以上作成する
- SSH公開鍵配布
  - ホストのfingerprintをDNSで配るかLDAPで配るか?
- sudoer配布
  - SSSDによるキャッシュが必須(RHEL 7.0+, 6.6+)

利用したい機能を決める(3/3)

- HBAC
  - RHEL 6.4から対応
- Active Directory とのCross realm trustによるWindowsからのSSO
  - ADとIdMは別のドメインである必要がある
- アプリケーションの認証統合
  - upstreamに連携用ドキュメントあり
    https://www.freeipa.org/page/HowTos
  - SaaS等の場合はRed Hat SSOなどを利用してOpenID ConnectやSAMLでの接続を検討する

NG集

- ロードバランサによる負荷分散はしない
  - 通常はDNSで行うので不要
  - DNSによるロードバランスを利用できない場合はクライアント側SSSDでサーバを列挙
- 1台だけで構築しない
  - IdMサーバ障害時に関連サービスでの新規ログインができなくなります
- ADや既存の他Kerberosと同じドメインにしない
- 一部のパッケージだけを更新しない。更新するときは関連する全てのパッケージを更新する。

関連資料

- RHEL 7ドキュメント「Linux ドメイン ID、認証、およびポリシーガイド」内 『パート II. Identity Management のインストール』
  - https://red.ht/2nHthSd

Thank You