

PRIMERGY RX300 上での Authentication Manager の動作検証と結果報告



富士通ソーシャルサイエンスラボラトリ



作成：2004年11月18日
株式会社 富士通ソーシャルサイエンスラボラトリ
テクマトリックス株式会社
RSA セキュリティ株式会社

PRIMERGY RX300 上での Authentication Manager の動作検証と結果

検証目的:

PRIMERGY RX300 上で RSA SecurID Authentication Manager の各コンポーネントである「Authentication Manager6.0」、「Domain Authentication Host」、「Domain Authentication Client」が正しく動作でき、かつサーバーセキュリティ強化のためサーバー(ドメインコントローラー)のローカルログインユーザに対しても SecurID 認証を行える事を検証目的としています。

場所:

FUJITSU IA Solution Center

日時:

2004/11/16(火)AM 10:00 ~ 10/17(水)AM 12:00

検証番号

2004-1116-02

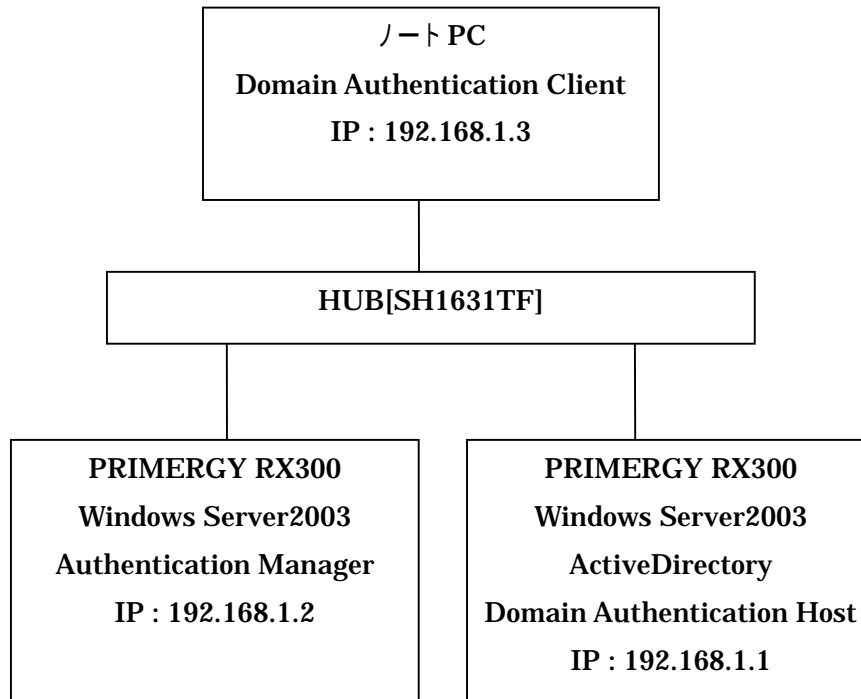
検証作業:

- ・株式会社富士通ソーシャルサイエンスラボラトリ
ネットワークシステム事業部 プロダクトビジネス部 恵美 玲央奈
- ・テクマトリックス株式会社
技術本部 ネットワーク技術部 セキュリティグループ 田中 亮達
技術本部 ネットワーク技術部 セキュリティグループ 山崎 優

ハードウェア構成状況 :PRIMERGY RX300 2台

RX300(スロット変換機構有)		標準構成	
		仕様	型名
CPU	CPU ソケット 1	Xeon3.2GHz/1MB	PGBF23P
	CPU ソケット 2	Xeon3.2GHz/1MB	PGBF23P
MEM	DIMM スロット 0A	1GB	PGBRU2T
	DIMM スロット 0A	1GB	
HDD	ベイ 1	73GB(U320, 15Krpm)	PG-HDH75K
5 インチベイ	ベイ 1	内蔵 CD-ROM ユニット	標準
FDD		内蔵 FDD ユニット	標準
LAN		標準 LAN ポート#0	

構成図



検証項目:

1. コンポーネント単体テスト
Authentication Manager と Domain Authentication Host を別筐体上に問題なくインストールできて、かつ問題なく単体で動作できる事をテストする。
2. サーバー(ドメインコントローラ)上のローカルログインユーザに対して認証テスト
PRIMERGY RX300(Windows Server 2003 ActiveDirectory)上のローカルログインユーザが対ログインする際にも SecurID 認証をかけてログインできる事をテストする。
3. ドメインクライアント認証テスト
ノート PC(ドメインクライアント)から、PRIMERGY RX300(Windows Server 2003 ActiveDirectory Domain Authentication Host)上を経由して、PRIMERGY RX300(Windows Server 2003 Authentication Manager 6.0)上との連携がとれ、認証ができるかテストする。
4. オフライン認証テスト
ネットワークに繋がっていない状態で認証を行い、正しく認証を行えるかテストする。

検証結果:

1. コンポーネント単体テスト

結果:

Authentication Manager と Domain Authentication Host は別筐体上に問題なくインストールできて、かつ問題なく単体で動作できる事を確認できました。

Authentication Manager6.0 のサービスは正常に起動されており各設定が行えることを確認。

Domain Authentication Host もインストール後、各設定が行えたことから PRIMERGY RX300 上、単体で動作できることを確認しました。

手順:

PRIMERGY 上にインストールされている Windows Server 2003 に ActiveDirectory を構築する。

各 PC をドメインに参加させ、名前解決ができていることを確認する。

ActiveDirectory 上で SecurID 認証用のグループとユーザを作成する。

ActiveDirectory が構築されていない筐体に Authentication Manager 6.0 をインストール

ActiveDirectory がインストールされている筐体に Certificate Utility をインストールして、各証明書を作成する。

同筐体に Domain Authentication Host をインストールする。

インストール後、Authentication Manager 6.0 のサービス起動確認、各設定を行う。

インストール後、Domain Authentication Host の各設定を行う。

2. サーバー(ドメインコントローラ)上のローカルログインユーザに対して認証テスト

結果:

PRIMERGY 上の Windows Server 2003 ActiveDirectory 上のローカルログインユーザに対してワンタイムパスワードを使用したセキュリティをかけることができ、かつログインの際にも問題なくワンタイムパスワードで認証できたことを確認しました。

手順:

ActiveDirectory 上で管理ツール->メインコントローラセキュリティポリシ->セキュリティの設定->ローカルポリシ->ユーザ権利の割り当て->「ローカルログオンを許可する。」からローカルログインさせるユーザまたはグループを追加する。

Domain Authentication Host 上で SecurID 認証をかけるグループを設定する。

PRIMERGY(ActiveDirectory)上でコントロールパネル->ACE/Agent->ドメインタブより、ローカルログインさせるグループを選択して、「Enable domain authentication for this client」にチェックを入れる。

同 PC 上でログオフして、ローカルログイングループに登録されているユーザでログインする。SecurID 認証がかけられておりワンタイムパスワードで認証ができログインできるこ

とを確認。

ログイン後、オフラインデータがダウンロードされていることを確認する。

3. ドメイン認証テスト

結果:

ドメインクライアント(ノート PC Domain Authentication Client)は、PRIMERGYRX300 上(Windows Server 2003 ActiveDirectory Domain Authentication Host)を通して PRIMERGY RX300 上への(Windows Server 2003 Authentication Manager 6.0)への連携環境で、問題なくワンタイムパスワードを使用してドメイン認証ができたことを確認しました。

手順:

ActiveDirectory 上より、コントロールパネル->ACE/Agent->Domain タブよりドメイン認証用のグループ

ープを選択する。

PRIMERGY(Windows Server 2003)にインストールされた Authentication Manager ともう片方の PRIMERGY(Windows Server 2003 ActiveDirectory)にインストールされた Domain Authentication Host で Proxy Agent 認証を行い連携ができているか確認する。

ドメインクライアント(ノート PC)に Domain Authentication Client をインストールする

ドメインクライアントから SecurID のワンタイムパスワードを使用してドメイン認証を行う。

認証ができたならば、オフラインデータがダウンロードされていることを確認する。

4. オフライン認証テスト

結果:

ネットワークに接続されていない状態でノート PC 上からワンタイムパスワードを使用してオフラインの状態でのログイン認証ができることを確認しました。

手順:

オフラインデータが存在することを確認する。

ドメインクライアント上でネットワークケーブルを外した状態にする。

一度クライアント上の PC でログオフする。

SecurID のワンタイムパスワードを使用してログインする。

以上の結果内容から、SecurID Authentication Manager の各コンポーネントは PRIMERGY RX300 上で問題なく動作し、かつサーバー(ドメインコントローラー)上のローカルログインユーザに対しても SecurID 認証が可能である。

以上

[お問い合わせ先]

- ・社名 : 株式会社 富士通ソーシャルサイエンスラボラトリ
- ・部署 : (二事本)NS) ネットワークインテグレーション部
- ・住所 : 〒211-0063
川崎市中原区小杉町 1-403武蔵小杉タワープレイス
- ・TEL : 044-739-1563
- ・FAX : 044-739-1597
- ・E-mail : ns-info@ssl.fujitsu.com
- ・URL : <http://www.ssl.fujitsu.com/>