以下の注をお読み下さい。View の設定がより簡単になります。

以下の言語でお読みいただけます:
Français Deutsch 简体中文 日本語 한국어

View 5.1 以降のリリースで変更があったので、従来よりも View コンポーネントの構成が若干異なっております。これらの注は、View 5.1 以降のリリースをインストールまたはアップグレードする時の落とし穴を避ける上で役立ちます。

注:View 5.1 から以降のリリースにアップグレードする場合、これらの構成手順を完了している必要があります。これらの注を使用して、View の手順を確認してください。

1) View 5.1 以降の接続サーバから以前のバージョンにダウングレードできません。

View 5.1 以降では、View LDAP 構成は暗号化され、View の以前のバージョンでは使用できません。

- View 接続サーバ インスタンスを View 5.1 以降にアップグレード後は、インスタンスを前バージョンにダウングレードできません。
- すべての View 接続サーバ インスタンスを複製されたグループ内でアップグレード後は、View の前バージョンを実行する他のインスタンスを追加できません。

注:ダウングレードはサポートされていなかったものの、過去のリリース版では対応されていました。今後は完全に無効になります。

2) vCenter Server および View Composer ホストには、有効な SSL 証明書が必要です。

- 最善の選択:vCenter Server および View Composer に Certificate Authority (CA) が提供する証明書があることを確認します:
    - vCenter Server がインストールされている Windows Server に CA が署名した SSL 証明書をインストールします。
    - View Composer で同じ作業を行います。同じホストに View Composer と vCenter Server をインストールする場合、同じ証明書を使用できますが、各コンポーネントで証明書を別々に構成する必要があります。

      * View Composer をインストールする前に証明書をインストールする場合、View Composer のインストール中に証明書を選択できます。

      * デフォルトの証明書を後で交換する場合、SviConfig ReplaceCertificate コマンドを実行して、新規証明書を View Composer で使用されたポートにバインドします。
    - 新規証明書の CA、および親 CA が View 接続サーバ インスタンスがインストールされている各 Windows サーバによって信頼されていることを確認してください。
- 代替の解決策:vCenter Server と View Composer を View に追加後、View Administrator の **[検証]** をクリックして View Composer のデフォルト証明書の拇印を承諾します。vCenter Server についても同じ操作を実行します。

詳細情報:View インストール ガイドの「View Servers の SSL 証明書の構成」を参照してください。

3) セキュリティ サーバおよび View 接続サーバ ホストには、有効な SSL 証明書が必要です。

- 最善の選択:View 接続サーバ インスタンスまたはセキュリティ サーバを Windows Server ホストにインストールした後、Windows Server 証明書ストアを開き、以下の手順を実行します。
    - CA によって署名され、クライアントが検証できる SSL 証明書をインポートします。
    - 中間証明書およびルート証明書を含む証明書チェーン全体がインストールされていることを確認します。
    - 証明書には秘密鍵があり、エクスポート可能としてキーにマーキングしていることを確認します。
    - vdm のように証明書に馴染みの名前を付けます。
- 代替の解決策:View server インストーラで Windows Server の証明書ストアにデフォルトの証明書を作成します。この証明書は自己署名されており、View Administrator では無効として表示されます。
- View 5.1 以降のリリースにアップグレード: 元の View servers に CA によって署名された SSL 証明書がある場合、操作は何も必要ありません。アップグレード時に View が Windows Server 証明書ストアに証明書をインポートします。

  オリジナルの View servers にデフォルトの証明書がある場合、View servers をアップグレードし、前述の最善の選択に従います。

詳細情報:View インストール ガイドの「View Servers の SSL 証明書の構成」を参照してください。

4) vCenter Server、View Composer、および View servers 用の証明書には、証明書失効リスト (CRL) を含める必要があります。

View は CRL なしで証明書を検証しません。

- 最善の選択:必要に応じて、これらの手順を行います:
    - CRL を証明書に追加します。
    - vCenter Server、View Composer、および View server ホストの Windows 証明書ストアにアップデートされた証明書をインポートします。
- 代替の解決策:CRL チェックを制御するレジストリ設定を変更します。

詳細情報:View インストール ガイドの「サーバ証明書で証明書失効チェックを構成」

注:インターネット アクセスのために社内でプロキシー設定を使用している場合、View 接続サーバ コンピュータを構成してプロキシー設定を使用できるようにする必要があります。この手順によって、インターネットの証明書失効チェック サイトにアクセスできます。Microsoft Netshell コマンドを使用して、プロキシー設定を View 接続サーバにインポートできます。

5) セキュリティが強化された Windows ファイアウォールが セキュリティ サーバと View 接続サーバ ホストで有効にする必要があります。

デフォルトでは、IPsec ルールによって、View セキュリティ サーバと View 接続サーバとの間の接続が管理され、[セキュリティが強化された Windows ファイアウォール] を有効にする必要があります。

- 最善の選択:View servers をインストールする前に、セキュリティが強化された Windows ファイアウォールを**オン**に設定します。アクティブ プロファイルで**オン**になっていることを確認し、さらに良いのは、すべてのプロファイルで**オン**に設定します。

- 代替の解決策:セキュリティ サーバをインストールする前に View Administrator を開き、グローバル設定、セキュリティ サーバ接続で IPsec を使用を**いいえ**に設定することで無効にします(これは推奨されません)。

6) IPsec をサポートするよう、バックエンド ファイアウォールを設定する必要があります。

セキュリティ サーバと View 接続サーバ インスタンスの間にバックエンドのファイアウォールを設定している場合、接続が有効になるようファイアウォール ルールを構成する必要があります。

詳細情報:View インストール ガイドの「IPsec をサポートするためにバックエンド ファイアウォールを構成」を参照してください。

7) View Client は View に接続するために HTTPS を使用する必要があります。

View接続サーバ インスタンスおよびセキュリティ サーバはクライアント接続のために SSL を使用します。

- View Client が中間デバイスをオフロードする SSL を介して接続する場合、中間デバイスの SSL 証明書を View 接続サーバまたはセキュリティ サーバにインストールする必要があります。

- ロード バランサーなどの中間デバイスを介して View Client が接続されるかどうかに関係なく、接続は HTTPS でなければなりません。中間デバイスを使用し、中間デバイスと View serverを HTTP(オフロードされた SSL)で接続したい場合、View server で locked.properties ファイルを構成します。

- HTTPS を使用しないように選択できる古い View Client では、HTTP をユーザーが選択するとエラーが発生します。これまでは、サイレントで HTTPS にリダイレクトされていました。SSL 接続を行うことができないクライアントは、View に接続できません。

詳細情報:View 管理ガイドの「中間サーバへのオフロードされた SSL 接続」を参照してください。

8) 暗号化されクリーンにされた View バックアップは新しい復元手順が必要です。

デフォルトでは、View 5.1 以降のバックアップが暗号化されます。View バックアップをクリーンするか(バックアップ データからパスワードおよび他の機密情報を除く)プレーン テキストでバックアップすることもできます(推奨されません)。

- 暗号化されたバックアップを復元するには、データを先に復号化する必要があります。View 接続サーバがインストールされている場合、指定したデータ リカバリ パスワードを使用する必要があります。

- クリーンにされたバックアップを復元しないでください。View LDAP 構成からパスワードなどのデータ

が消えてしまいます。このデータがなければ、View コンポーネントは正常に機能しません。通常の機能を復元するには、View Administrator を使用して、すべてのパスワードおよび他の欠落しているデータ項目を手動でリセットする必要があります。

詳細情報:View 管理ガイドの「View 構成データのバックアップと復元」を参照してください。

9) View 5.1 以降のセキュリティ サーバをアップグレードまたは再インストールできる前に、ペアになっている View 接続サーバ インスタンスから関係する IPsec ルールを削除する必要があります。そうすれば、新しいルールを確立できます。

- View Administrator でセキュリティ サーバを選択し、**[その他のコマンド] -> [アップグレードまたは再インストールを準備]**をクリックします。

  注:サーバをアップグレードまたは再インストールする前に、セキュリティ サーバを View から削除する必要はありません。

詳細情報:View インストール ガイドの「セキュリティ サーバのアップグレードまたは再インストールを準備」を参照してください。