阅读以下说明，轻松设置 View！

本说明提供以下语言版本：
Français Deutsch 简体中文 日本語 한국어

我们在 View 5.1 及后续版本中所做的更改要求您按与以往略有不同的方式配置 View 组件。阅读以下说明有助您避免在安装或升级到 View 5.1 或更高版本时出现潜在的错误。

注意：从 View 5.1 升级到更高版本时，您应当已经执行下述配置步骤。请根据以下说明检查您的 View 设置。

1) 无法将 View 5.1 或更高版本的连接服务器降级到早期版本。

在 View 5.1 或更高版本中，View LDAP 配置经过加密，早前版本的 View 无法使用。

- 将 View 连接服务器实例升级到 View 5.1 或更高版本后，无法再将该实例降级到早期版本。
- 升级副本组中的全部 View 连接服务器实例后，无法再添加运行早期版本 View 的实例。

注意：降级操作始终不受支持，但在之前版本中却可行。现在，此操作不可行了。

2) vCenter Server 和 View Composer 主机需要有效的 SSL 证书。

- *最佳选择*：确保 vCenter Server 和 View Composer 具备由证书颁发机构 (CA) 提供的证书：
    - 在装有 vCenter Server 的 Windows Server 上安装由 CA 签发的 SSL 证书。
    - 针对 View Composer 执行相同的操作。如果将 View Composer 和 vCenter Server 安装在同一台主机上，则它们可以使用同一证书，但您需要单独为每个组件配置证书。

      * 如果是在安装了证书后才安装 View Composer，则您可以在安装 View Composer 期间选择该证书。

      * 如果之后要替换默认证书，请运行 *SviConfig ReplaceCertificate* 命令将新证书绑定至 View Composer 使用的端口。
    - 请确保新证书的 CA 和任何父 CA 受安装了 View 连接服务器实例的 Windows Server 的信任。
- *备用方法*：在为 View 添加 vCenter Server 和 View Composer 后，通过单击 View Administrator 中的**验证**，接受 View Composer 的默认证书指纹。对 vCenter Server 执行同样的操作。

详细信息：请参阅《View 安装指南》中的“为 View Server 配置 SSL 证书”。

3) 安全服务器和 View 连接服务器主机需要有效的 SSL 证书。

- *最佳选择*：在 Windows Server 主机上安装 View 连接服务器实例或安全服务器后，打开 Windows Server 证书存储区并执行以下步骤：
    - 导入由 CA 签发且您的客户端可以验证的 SSL 证书。
    - 请确保安装了整个证书链，包括中间证书和根证书。

- 请确保证书具有一个私钥，而且您将该密钥标记为可导出。
- 将证书的友好名称改为 *vdm*。

- *备用方法*：让 View Server 安装程序在 Windows Server 证书存储区中创建一个默认证书。该证书为自签名证书且将在 View Administrator 中显示为无效。
- *升级到 View 5.1 或更高版本*：如果原始 View Server 已具有由 CA 签发的 SSL 证书，则您无需执行任何操作。在升级期间，View 会将证书导入 Windows Server 证书存储区。

  如果原始 View Server 有默认证书，请升级 View Server，然后执行上述*最佳选择*步骤。

详细信息：请参阅《View 安装指南》中的“为 View Server 配置 SSL 证书”。

4) vCenter Server、View Composer 和 View Server 的证书必须包含证书撤消列表 (CRL)。

View 将不会验证没有提供 CRL 的证书。

- *最佳选择*：如果需要，请执行以下步骤：
  - 为证书添加 CRL。
  - 将更新的证书导入 vCenter Server、View Composer 和 View Server 主机上的 Windows 证书存储区。
- *备用方法*：更改用于控制 CRL 检查的注册表设置。

详细信息：请参阅《View 安装指南》中的“配置服务器证书上的证书撤消检查”。

注意：如果贵公司为 Internet 访问使用代理设置，可能需要将 View 连接服务器计算机配置为使用这些代理设置。此步骤可确保服务器能够访问 Internet 上的证书撤消检查站点。您可以使用 Microsoft *Netshell* 命令将代理设置导入到 View 连接服务器。

5) 安全服务器和 View 连接服务器主机上必须已启用“高级安全 Windows 防火墙”。

默认情况下，IPsec 规则会控制 View 安全服务器与 View 连接服务器之间的连接并且会要求启用“高级安全 Windows 防火墙”。

- *最佳选择*：请先将“高级安全 Windows 防火墙”设置为**打开**，然后再安装 View Server。请确保它对于任何活动配置文件均设置为**打开**；最好是对于*所有*配置文件都将其设置为**打开**。
- *备用方法*：在安装安全服务器之前，请打开 View Administrator 并通过将*使用 IPsec 进行安全服务器连接*设置为**否**禁用全局设置。（不推荐。）

6) 后端防火墙必须设置为支持 IPsec。

如果安全服务器和 View 连接服务器实例之间存在后端防火墙，您必须配置防火墙规则以允许连接正常工作。

详细信息：请参阅《View 安装指南》中的“配置后端防火墙以支持 IPsec”。

7) View Client 必须使用 HTTPS 连接到 View。

View 连接服务器实例和安全服务器使用 SSL 进行客户端连接。

- 如果 View Client 通过一个 SSL 卸载中间设备连接，您必须在 View 连接服务器或安全服务器上安装该中间设备的 SSL 证书。
- 无论 View Client 是否通过负载平衡器等中间设备连接，该连接都必须为 HTTPS。如果您使用了中间设备且希望中间设备和 View server 之间的连接基于 HTTP（SSL 卸载），请配置 View server 上的 *locked.properties* 文件。
- 如果用户选择 HTTP，则可选择不使用 HTTPS 的较早版本的 View Client 将出错。以前，它们会默认重定向到 HTTPS。不能建立 SSL 连接的客户端将无法连接到 View。

详细信息：请参阅《View 管理指南》中的“卸载 SSL 连接至中间服务器”。

8) 经加密和清理的 View 备份需要新的恢复步骤。

默认情况下，View 5.1 或更高版本的备份经过加密。您还可以清理 View 备份（从备份数据中排除密码和其他敏感信息）或以纯文本格式进行备份（不推荐）。

- 要恢复经加密的备份，您必须先对数据进行解密。您必须使用在安装 View 连接服务器时提供的数据恢复密码。
- 请勿恢复清理后的备份。View LDAP 配置中将缺少密码等数据。缺少该数据，View 组件将无法正常运行。要恢复正常功能，您需要使用 View Administrator 手动重置所有密码和其他缺少的数据项。

详细信息：请参阅《View 管理指南》中的“备份和还原 View 配置数据”。

9) 在升级或重新安装 View 5.1 或更高版本安全服务器之前，您必须从配对的 View 连接服务器实例中移除相关 IPsec 规则，以便可以建立新规则。

- 在 View Administrator 中，选择该安全服务器，然后单击**更多命令 > 准备升级或重新安装**。

  注意：在升级或重新安装服务器之前，您无需从 View 移除安全服务器。

详细信息：请参阅《View 安装指南》中的“准备升级或重新安装安全服务器”。