NetBackup IT Analytics 安全和加密参考

版本：11.4

VERITAS
now part of Cohesity

NetBackup IT Analytics 安全和加密参考

上次更新时间： 2025-03-25

法律声明

Cohesity, Inc.
2625 Augustine Drive.
Santa Clara, CA 95054

http://www.veritas.com

技术支持

技术支持具有全球性支持中心。所有支持服务将会根据您的支持协议以及当时最新的企业技术支持政策进行交付。有关支持产品和服务以及如何联系技术支持的信息，请访问我们的网站：

https://www.veritas.com/support

您可以在下列 URL 上管理 帐户信息：

https://my.veritas.com

如果您对现有支持协议有疑问，请通过以下方式联系您所在地区的支持协议管理部门：

全球（日本除外）	CustomerCare@veritas.com
日本	CustomerCare_Japan@veritas.com

文档

请确保您的文档是最新版本。每个文档都在第 2 页上显示上次更新日期。最新的文档可在 网站上找到。

Services and Operations Readiness Tools (SORT)

Services and Operations Readiness Tools (SORT) 是一个网站，提供的信息和工具有助于自动处理及简化某些耗时的管理任务。根据具体产品，SORT 会帮助您准备安装和升级、识别您数据中心的风险并提高操作效率。要了解 SORT 为您的产品提供了哪些服务和工具，请参见数据表：

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

目录

1

NetBackup IT Analytics 组件和安全遵从性

本章节包括下列主题：

概述

本文档介绍了 Veritas NetBackup IT Analytics 所遵循的各种安全标准和数据加密方法。由于该产品必须探测多个基础架构节点和数据点来收集数据，因此在数据收集、存储和处理的各个阶段都遵循严格的安全标准和加密准则。此外，本文档还讨论了在修复产品问题和开发新功能期间遵循的内部安全标准和做法。

NetBackup IT Analytics 的组件

NetBackup IT Analytics 包括以下组件：

1. 门户服务器：安装了 NetBackup IT Analytics 门户服务器软件的物理服务器
2. 门户服务器软件：从报告数据库检索和呈现报告数据所需的二进制文件、SQL 脚本、配置文件以及开源软件或第三方软件产品。
3. 报告数据库：存储所有报告数据的 Oracle 数据库。它通常安装在门户服务器上，但如果需要，也可以安装在单独的专用数据库服务器上。这些二进制文件是在安装过程的第一步安装的。
4. Data Collector：收集有关备份服务器和存储阵列报告数据的软件。Data Collector 通常安装在单独的服务器上。

5. IT Analytics Exporter：该软件提供了一种额外的导出机制，用于从 NetBackup 资源监视器收集数据，以及通过计算资源从操作系统和硬件指标数据收集数据。

遵从美国联邦政府标准

NetBackup IT Analytics 遵从以下美国联邦政府标准：

- 加密：NetBackup IT Analytics 使用 FIPS 140-2 加密库进行静态数据加密和传输中数据加密。但是，不启用对 FIPS 140-2 的完全支持。
- 通信和数据传输：NetBackup IT Analytics 遵从 IPv4 和 IPv6 要求，从而通过公用网络和专用网络安全地传输数据。联网系统之间的通信遵循 SSL/TLS 协议。支持 TLS 1.2 和 TLS 1.3。
- 网络安全：NetBackup IT Analytics 遵循公钥基础架构 (PKI) 和双重身份验证要求，以确保网络安全。可将网络配置为需要单点登录 (SSO)，以便 NetBackup IT Analytics 继承 SSO 的 PKI 或双重身份验证。
- 在 Linux 上，如果已对 RHEL 进行配置且符合 STIG 规范，则 RHEL 支持 NetBackup IT Analytics。该产品的 Apache、Oracle 和 Tomcat 子系统也符合 STIG 规范。所有 1 类项目以及某些 2 类和 3 类项目均满足应用程序安全和开发要求。
- 安全技术实施指南 (STIG)：符合 STIG 规范的 RHEL 支持 NetBackup IT Analytics。此外，Apache、Oracle 和 Tomcat 子系统也符合 STIG 规范。应用程序安全和开发要求遵循 CAT 1 STIG 合规性级别。
- NetBackup IT Analytics 静态数据安全：希望对存储在 Oracle 数据库中的 NetBackup IT Analytics 数据静态加密的 NetBackup IT Analytics 用户必须使用透明数据加密 (TDE) 这一 Oracle 功能。TDE 是 Oracle Advanced Security 的一部分。它以 Oracle Database Enterprise Edition 的附加许可选件的形式提供。

2

用户身份和访问管理

本章节包括下列主题：

概述

此部分介绍了 NetBackup IT Analytics 中的用户创建和用户基于角色的访问权限。此部分还介绍了产品支持的安全访问方法。

关于用户类型

共有三种门户用户类型：

表 2-1 用户类型

用户类型	权限
管理员	在管理员的已分配组中或下级组中，管理用户帐户和设置主机组。管理员可以创建“最终用户”帐户和“管理员”帐户，但只能在管理员的主组中创建。 在MSP（托管服务提供商）环境中，每个客户端都具有“管理员”帐户，这些帐户仅有权访问该客户端的域以及该域中的主机组。 **注意：**门户升级将自动为所有管理员启用新添加报告的权限，并显示“**清单**”视图，包括所有对象。有关特定产品版本中引入的报告和功能的列表，请参考版本说明。
超级用户	任何其他用户均无法修改此用户可用的权限。 超级用户权限高于管理员用户权限，可以执行以下操作： ■ 从上到下访问整个门户主机组层次，无需考虑用户的组分配。 ■ 管理 Oracle 表空间。 ■ 定义和管理服务器备份周期。 ■ 为主机组层次内的任何组创建“最终用户”帐户和“管理员”帐户。 ■ 访问所有默认报告和用户生成的报告。 ■ 当系统报告模板可用时，查看其中的“**新建**”和“**更新**”标记。 ■ 模拟用户配置文件。
最终用户	■ 管理员已授予权限的功能。最终用户可使用的权限不能超过其所属主组的权限。 ■ 最终用户只能在用户自己的主组（域）内创建“最终用户”帐户。

用户组

用户组是一次性管理大量用户的有效方法。管理员可以为一个组分配权限，然后这些权限即会传播到该组中的用户。例如，权限如下：

- 启用对特定报告的访问权限
- 启用对功能区的访问权限
- 限制对门户特定页面的访问权限

域

利用域可以将报告数据库“分区”为单个私有领域。它主要用于为多租户系统实施安全控制，并且它是与主机组层次顶层关联的唯一实体。域名在安装过程中提供，门户将其分配给根文件夹。

Data Collector 使用域进行：

- 身份验证：主服务器记录必须存在于域的主机组层次中。（仅限 Veritas NetBackup）
- 主机搜索：Data Collector 搜索域的主机组层次，以检查与其所收集的备份数据相关联的主机。如果找不到主机，则将新主机添加到域的根级别主机组文件夹中。

企业环境通常只有一个域。添加（或删除）主机组或属性时，将对域及其所有主机组进行全局操作。除非您是托管服务提供商 (MSP)，否则，在通过门户添加或删除主机组或属性时，不必指定域。

多域

如果您是托管服务提供商，则必须能够管理多个独立层次，每个客户公司一个层次。作为 MSP，您将为每个客户定义一个唯一的域。添加或删除属性时，可以对所有域执行此操作，也可以选择特定域来应用更改。

域与主机组层次关联，所有新发现的主机均将添加到与此域关联的根主机组。每个 MSP 客户将拥有一个具有自己层次的单独域。

注意：主机组只能用作一个域的根。例如，可以为 Acme Corp 定义一个主机组，然后创建一个 Acme 域，而此域使用主机组作为其主机组层次的根。域与主机组关联后，此主机组不能成为任何其他域的根。

通过单点登录 (SSO) 进行用户身份验证

NetBackup IT Analytics 支持使用单点登录 (SSO) 进行标准的统一登录。通过外部身份管理服务器执行用户身份验证，从而提高用户密码和身份详细信息的安全级别。因此，单点登录需要启用了 SSL 的 NetBackup IT Analytics 门户、外部身份提供程序 (IDP) 和外部 LDAP 目录。

单点登录 (SSO) 前提条件

- 必须使用具有以下属性的 SSL 证书为 NetBackup IT Analytics 门户启用 SSL（https 协议）：
  - 签名算法名称：SHA256 with RSA
  - 主题公钥算法：2048 位 RSA 密钥
- 支持 SAML 2.0 的外部身份提供程序 (IDP)

- 必须使用 Keystore 实用程序 (deployCert) 将 SSL 证书添加到门户 Keystore 中

设置外部身份提供程序 (IDP) 服务器

为使 IDP 与 NetBackup IT Analytics 门户进行通信，需在外部服务器上配置 LDAP 目录以进行用户管理。必须为将要登录门户的每个用户填充某些属性。用户还必须至少属于一个组。

外部 LDAP 目录中的用户和组

在外部 LDAP 目录中为每个用户设置以下属性。对于每个属性，必须存在 **name** 和 **friendlyName** 属性并且已填充值。这些属性必须同时由外部 LDAP 目录和 IDP 服务器公开。属性的名称如下：

- displayName：<first_name> <last_name>，例如 Jane Smith
- email：电子邮件地址
- mobile：手机号码
- telephoneNumber：工作电话或住宅电话号码
- sAMAccountName：用作登录名的唯一用户名
- memberOf：用户所属的组名称列表。

注意：属性 `memberOf` 需要对 Microsoft Azure IDP 进行自定义。建议为“memberOf”属性设置“**分配给应用程序的组**”，而不是“**所有组**”或“**安全组**”。有关更多详细信息，请单击此处。

外部用户必须属于一个外部目录组，且该目录组也作为用户组存在于 NetBackup IT Analytics 门户之中，只有在这种情况下外部用户才可以使用 SSO 登录门户。如果满足设置条件，则用户首次登录门户时，用户配置文件将从外部目录进行同步。用户还将继承分配给该用户组的所有权限。

在 IDP 服务器中注册

在 NetBackup IT Analytics 门户与 IDP 服务器之间交换元数据 XML 文件，可以实现注册过程。在门户端，只要配置了 SSO 并重新启动 Portal Tomcat 服务，就可以下载元数据 XML 文件并将其提供给 IDP 服务器。此文件包含 SSL 证书，并可将 NetBackup IT Analytics 标识为 SSO 的服务提供程序。必须从 IDP 服务器下载相似的元数据 XML 文件并将其提供给门户。

请参见《NetBackup IT Analytics 系统管理指南》中的“使用安全声明标记语言 (SAML) 配置单点登录 (SSO)”。

AD/LDAP 配置

NetBackup IT Analytics 支持用户身份验证，还支持使用 Active Directory (AD) 或轻量型目录访问协议 (LDAP) 进行授权。

AD/LDAP 身份验证和授权的配置通过 `portal.properties` 文件的配置参数来完成。

AD/LDAP 配置属性

AD/LDAP 配置支持以下属性，可以在 `portal.properties` 文件中进行设置。

操作系统特定的 `portal.properties` 文件位置：

- Linux：`/opt/aptare/portalconf/portal.properties`
- Windows：`C:\opt\aptare\portalconf\portal.properties`

表 2-2 AD/LDAP 配置属性

属性	说明
ldap.enabled	要启用 LDAP，将此属性设置为 true。 支持的值：true | false
ldap.searchBase	■ 从中执行搜索以在身份验证目录中查找用户的位置。 ■ 通常称为 Active Directory (AD) 搜索库，这是 Active Directory 树中用于搜索 LDAP 用户的起点。此搜索库采用 LDAP 可分辨名称格式，包含完全限定域名。NetBackup IT Analytics 仅支持一个搜索库。 示例：`dc=example,dc=company,dc=com`
ldap.url	■ 设置为 AD 的主机和端口。请注意，此 URL 值的前缀为 **ldap:**。如果使用 SSL，将前缀更改为 ldaps。 ■ 如果对外部 LDAP 配置使用 Active Directory，则可能需要使用全局编录端口 3268，而不使用端口 389。 ■ 如果使用 SSL，则可以对标准 LDAP 使用安全全局编录端口 3269 或 636。 示例：`ldap://example.company.com:389` 或 `ldaps://example.company.com:636`

属性	说明
ldap.dn	■ 设置为有权搜索 SEARCHBASE 的用户的 ID。此用户必须能够搜索所有 LDAP 目录服务器。 ■ NetBackup IT Analytics 要求用户有权在 Active Directory 结构中的基本 DN（可分辨名称）下进行搜索。此用户必须是具有管理权限的帐户，通常为管理员。可以是在安装 Active Directory 时创建的管理员帐户，也可以是已经创建，又被授予管理权限或置于具有管理权限的组中的帐户。 ■ 如果使用 Active Directory，请指定此设置，因为 Active Directory 服务不允许匿名绑定。Microsoft Active Directory 需要提供可搜索 LDAP 目录权限的用户的用户名和密码。 示例： `ldap.dn =CN=Admin,CN=Users,DC=example, DC=company,DC=com`
ldap.password	设置为 ldap.dn 属性中使用的用户的密码。配置 LDAP 后，重新启动 Portal Tomcat 服务时，将清空该值，并在 `ldap.password.encrypted` 属性中设置加密值。
ldap.password.encrypted	配置 LDAP 后重新启动 Portal Tomcat 服务时设置此属性。此属性的值为 `ldap.password` 属性的加密值。
ldap.loginAttribute	用于身份验证的登录属性。Active Directory 中用于指定用户名的属性名称，如 *uid* 或 *sAMAccountName*。 示例： `ldap.loginAttribute=sAMAccountName`
ldap.authorization	如果设置为 true，则门户为用户授予 AD 组的权限。 在门户中，必须至少将一个新用户所属的 AD 组配置为用户组。 **注意：** 如果 AD 组未与门户中的用户组建立映射，登录期间，身份验证将失败，显示错误“外部 LDAP 用户不存在用户组映射”。 支持的值：true | false

属性	说明
ldap.newUserDomain	创建新用户的门户域名。仅在 `ldap.authorization` 设置为 true 时使用。 要在门户中查找域名，请导航到“管理”>“域”>“域名” 示例： `ldap.newUserDomain=example.company.com`
ldap.keystore	如果为 LDAP 启用了 SSL 支持，则必须： ■ 包含 AD 证书所在的 keystore 路径位置 ■ aptare:tomcat 权限 **注意：**如果没有为 LDAP 启用 SSL，则必须将其注释掉。
ldap.keystore.password	在 `ldap.keystore` 属性中设置的 keystore 密码。配置 LDAP 后，重新启动 Portal Tomcat 服务时，将清空该值，并在 `ldap.keystore.password.encrypted` 属性中设置加密值。 **注意：**如果没有为 LDAP 启用 SSL，则必须将其注释掉。
ldap.keystore.password.encrypted	配置 LDAP 后重新启动 Portal Tomcat 服务时设置此属性。此属性的值为 `ldap.keystore.password` 属性的加密值。 **注意：**如果没有为 LDAP 启用 SSL，则必须将其注释掉。
ldap.disable.user.attribute.name （从 11.0 开始提供）	其值为 AD 属性，表示用户是处于活动状态还是非活动状态。通过 AD 进行门户身份验证期间，REST API 使用分配给此属性的 AD 属性来检查用户是否仍然是活动的 AD 用户。 例如，如果 `ad.user.active` 是表示用户是处于活动状态还是已禁用状态的 AD 属性，则必须分配 `ad.user.active` 作为该属性 (`ldap.disable.user.attribute.name=ad.user.active`) 的值。

属性	说明
ldap.disable.user.attribute.value （从 11.0 开始提供）	其值必须与 AD 属性的值（在 `ldap.disable.user.attribute.name` 中指定）相同，该值表示 AD 用户处于已禁用状态。 例如：如果 `ad.user.active` 是 AD 中用户状态的属性，它可能具有多个值，如 `live`、`inactive`、`joined` 等。如果值 `inactive` 表示用户在 AD 中处于已禁用状态，则必须将此属性 (`ldap.disable.user.attribute.value=inactive`) 的值设置为 `inactive`。 REST API 将此值与 `ldap.disable.user.attribute.name` 属性中指定的 AD 属性值进行匹配。如果值匹配，则表示已在 NetBackup IT Analytics 门户上禁用该用户。 **注意：** 门户超级用户必须明确激活已在 AD 和门户中停用但仅在 AD 中重新激活的用户。具有足够权限的门户管理员也可以激活此类用户。如果不进行用户激活，门户访问将受到限制。

要配置 AD/LDAP 进行用户身份验证和授权，门户管理员必须至少在门户中创建一个用户组，该用户组也作为 UserGroup 出现在 AD/LDAP 中。

支持 LDAP over SSL

如果使用的是自签名证书或来自非标准证书颁发机构 (CA) 的 AD 证书，则需要具有 AD 证书的 Keystore 并更新 `portal.properties` 文件中的 LDAP 配置。如果使用的是 CA 的标准证书，则可以跳过此过程。

3

数据安全和加密

本章节包括下列主题：

数据收集器安全和数据加密

数据收集器提供非对称加密，又称“公钥加密”。使用这种加密形式时，密钥成对提供，一个密钥进行加密，只有另一个密钥可以解密。在收集数据时，这种加密方法提供额外的安全性。

在升级方案中，您必须通过生成密钥文件来启用非对称加密，从而提高安全性。您也可以选择继续使用对称加密方法，但其安全性低于非对称加密。在升级后，或者在出现数据损坏或密钥丢失之类的问题时，可以随时生成密钥文件。

要在全新安装或升级方案中使用此功能，必须在门户中手动生成密钥文件。在门户中添加数据收集器时，下载密钥，然后在收集器服务器上安装数据收集器软件时指向该位置。对于现有数据收集器，可以随时为非对称加密生成密钥。您可以选择加密/解密凭据。

为 File Analytics 设置符合 FIPS 的数据收集器

要符合 FIPS 140-2，必须按照以下建议为 File Analytics 配置数据收集器：

1. 要启用 FIPS 遵从性，必须在符合 FIPS 的系统上安装数据收集器。
2. 确保数据收集器和目标 Windows 文件服务器均在 FIPS 模式下配置。

3. 指定 **vers=2** 作为收集器和目标系统之间使用的协议版本。
4. 确保在目标系统上使用 Kerberos 身份验证。

注意：在 FIPS 和 Kerberos 中设置 Windows 文件服务器的步骤超出了本文档的范围。要了解相关步骤，您可以参考相关的产品文档。

数据库安全性

Oracle 数据库存储所有报告数据。报告数据库通常安装在门户服务器上，但也可以轻松安装在单独的服务器上，最好是一台专用数据库服务器。这些二进制文件是在安装过程的第一步安装的。

通过自动运行清除脚本可管理报告数据库中的数据，清除脚本将就不同产品乃至不同数据类型的数据特定保留期限自动运行。某些报告在获得历史数据的访问权限后更具价值。因为报告数据库仅存储元数据，所以报告数据库上的数据量相对较小 (GB)。

用户的 Oracle 安全配置文件

根据 Oracle 的建议，用户配置文件 ORA_STIG_PROFILE 将应用于所有用户帐户，除非使用限制性更强的配置文件。

下面给出了一些查询，用于检索有关用户配置文件的更多信息。

- 要查看 PORTAL 和 APTARE_RO 用户使用的配置文件并查看这些配置文件下的资源属性，请使用以下查询：

```
SELECT du.USERNAME, dp.PROFILE, du.ACCOUNT_STATUS, dp.*
FROM DBA_USERS du, DBA_PROFILES dp
WHERE du.username IN ('PORTAL', 'APTARE_RO')
AND du.profile = dp.profile
ORDER BY USERNAME;
```

- 要查看可能使用的所有可用用户配置文件的详细信息，请使用以下查询：

```
SELECT * FROM DBA_PROFILES;
```

要将配置文件分配给现有用户或创建新配置文件，请参见 Oracle 文档的 Creating a Profile 部分。

注意：如果对为 PORTAL 和/或 APTARE_RO 分配的用户配置文件进行了任何更改，则可能会根据新配置文件的限制强制更改这些用户的现有密码。如果随后更改了这些用户的密码，则必须在应用程序中进行更新。

NetBackup IT Analytics 静态数据安全

希望对存储在 Oracle 数据库中的 NetBackup IT Analytics 数据静态加密的 NetBackup IT Analytics 用户可以尝试透明数据加密 (TDE) 这一 Oracle 功能。TDE 是 Oracle Advanced Security 的一部分。它以 Oracle Database Enterprise Edition 的附加许可选件的形式提供。

TDE 对业务应用程序透明，不需要更改应用程序。在数据库存储级别进行加密和解密，对应用程序使用的 SQL 界面（无论是入站 SQL 语句，还是出站 SQL 查询结果）没有任何影响。

Oracle 使用 TDE 对数据进行静态加密。如果 Oracle 数据库数据文件的存储介质被盗，TDE 有助于保护介质上存储的数据。

数据库连接属性

下表汇总了门户使用的 Oracle 用户和密码的 portal.properties 值。

表 3-1 门户属性及说明。

门户属性	说明
db.driver	此值是由门户安装程序自定义，不应修改。
db.url	这是 NetBackup IT Analytics 数据库所在的地址。取决于安装过程中所输入的内容。主机名更改时，可能需要对此值进行修改。
db.user	使用此属性可更改用于登录访问数据库的数据库用户 ID。默认值为 **portal**。
db.password db.password.encrypted=	输入要与数据库用户配合使用的密码。默认值为 **portal**。密码最初以明文形式存储，但在重新启动 Tomcat 门户服务之后，密码将以加密格式保存，并且会从 portal.properties 中删除明文密码。
db.connection.max	使用此属性可指定允许的最大数据库连接数。默认值为 25。
db.connection.min	使用此属性可指定门户可以具有的最小数据库连接数。默认值为 25。
db.connection.expiration	当门户报告启动长时间运行的数据库查询时，此值（以分钟为单位）用于确定在查询花费太长时间无法完成时报告将在何时超时。默认值为 5。
db.ro_user_password db.ro_user_password.encrypted=	输入要与数据库只读用户配合使用的密码。默认值为 **aptaresoftware123**。密码最初以明文形式存储，但在重新启动 Tomcat 门户服务之后，密码将以加密格式保存，并且会从 portal.properties 中删除明文密码。
db.ro_user_password db.ro_user_password.encrypted=	用于 NetBackup IT Analytics 数据库表的 Oracle 数据库只读用户密码。预设值为 aptaresoftware123。
db.sysdba_user	NetBackup IT Analytics 数据库表的 Oracle 数据库系统 DBA。预设值为 system。

修改 Oracle 数据库用户密码

使用以下实用程序修改 Oracle 数据库用户 **portal** 和 **aptare_ro** 的密码。这些说明仅适用于用户 **portal** 和 **aptare_ro**。

- Linux：/opt/aptare/utils/changeDBPassword.sh
- Windows：C:\opt\aptare\utils\changeDBPassword.bat

新密码不能包含以下字符：

- 双引号 '"'。
- 反斜杠 '/'。
- 空格 ' '。
- 重音符 '`'

注意：如果启用了 CyberArk 功能，请勿修改 Oracle 数据库密码。

完成以下步骤可以修改 Oracle 数据库用户的密码。这些说明适用于 aptare_ro 和 portal 用户。

1 在 Linux 上使用 root 访问权限登录，或者在 Windows 上使用管理员访问权限登录。

2 停止门户和代理 Tomcat 服务。

3 更改用户密码：

在 Linux 上：

```
/opt/aptare/utils/changeDBPassword.sh -user <user_name>
<password>
```

在 Windows 上：

```
C:\opt\aptare\utils\changeDBPassword.bat -user <user_name>
<password>
```

这会更新 Oracle 配置中指定用户的密码，以及 `portal.properties` 和 `datrarcvrproperties.xml` 等属性文件。

4 更改密码后，立即重新启动 File Analytics 服务。

子系统与 Data Collector 之间的通信加密

请参考此表，检查 Data Collector 是否使用加密通信与目标子系统进行通信。

模块：存储

表 3-2 与存储系统通信

子系统	通信	协议	端口
Dell Compellent	已加密	SMI-S 基于 https	5989
Dell EMC Elastic Cloud Storage (ECS)	已加密	https	4443
Dell EMC Unity	已加密	https	443、8443
EMC Data Domain Storage	已加密	SSH	22
EMC Isilon	已加密	SSH	22
EMC Symmetrix	基于 FC	-	-
EMC VNX (CLARiiON)	已加密	https	443
EMC VNX (Celerra)	已加密	https	443
EMC VPLEX	已加密	https	443
EMC XtremIO	未加密	http	80
HP 3PAR	已加密	SSH	22
HP EVA	已加密	https	443
HPE Nimble Storage	已加密	https	可配置
Hitachi Block Storage	未加密	TCP	2001
Hitachi Content Platform (HCP)	已加密	https	9090
Hitachi NAS	已加密	ssc	206
Hitachi Vantara 全闪存和混合闪存存储	已加密	https	23451、22016

子系统	通信	协议	端口
IBM Cloud Object Storage	已加密	https	443
IBM Enterprise	未加密	TCP	1751、1750、1718
IBM SVC	已加密	SSH	22
IBM XIV	已加密	SSH	22
Microsoft Windows Server	已加密	WMI	NTLM/ Kerberos/ PktPrivacy
NetApp	已加密	https	443
NetApp 群集模式	已加密	https	443
NetApp E 系列	已加密	SMCli	-
Pure Storage FlashArray	已加密	https	443
Veritas NetBackup Appliance	已加密	WMI 代理	-

模块：网络和 Fabric

表 3-3 与网络系统通信

子系统	通信	协议	端口
Brocade 交换机	已加密	https	443（可配置）
Brocade 区域别名	已加密	https	443（可配置）
Cisco 交换机	已加密	https	5989
Cisco 区域别名	已加密	https	5989

模块：虚拟化

表 3-4 与虚拟化技术通信

子系统	通信	协议	端口
IBM VIO	已加密	SSH telnet	22 23

子系统	通信	协议	端口
Microsoft Hyper-V	已加密	WMI	NTLM/ Kerberos/ PktPrivacy
VMware	已加密	https	443

模块：File Analytics

表 3-5 与文件管理系统通信

子系统	通信	协议	端口
File Analytics	已加密	NTLM	443

模块：同步复制

表 3-6 与同步复制系统通信

子系统	通信	协议	端口
NetApp	已加密	https	137 和 139

模块：云

表 3-7 与云技术通信

子系统	通信	协议	端口
Amazon Web Service	已加密	https	443
Microsoft Azure	已加密	https	443
OpenStack Ceilometer	已加密	https	35357
OpenStack Swift	已加密	https	35357（管理端口） 5000（默认公用端口）

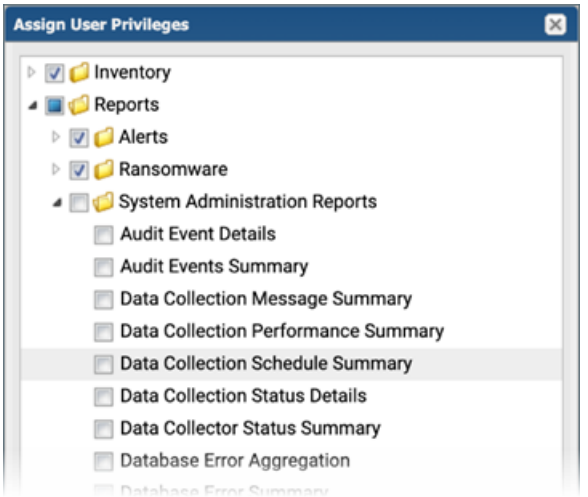
模块：数据保护

表 3-8 与数据保护技术通信

子系统	通信	协议	端口
Cohesity DataProtect	已加密	https	443
Commvault Simpana	已加密	WMI 代理	-
Dell EMC Networker Backup & Recovery	已加密	https	9090
EMC Avamar	已加密	SSH	22
EMC Data Domain Backup	SSH	SSH	22
EMC NetWorker	SSH	SSH	22
HP Data Protector	SSH	SSH	22
IBM Spectrum Protect (TSM)	未加密	TCP	1500
IBM Spectrum Protect Plus	已加密	https	443
NAKIVO Backup & Replication	已加密	https	443
Oracle Recovery Manager (RMAN)	未加密	jdbc	1521
Rubrik Cloud Data Management	已加密	https	443
Veeam Backup & Replication	已加密	wmi	NTLM/ Kerberos/ PktPrivacy
Veritas NetBackup	可配置	SSH	22

报告安全性

管理员可以通过 NetBackup IT Analytics 中的系统控制板管理报告查看与整个 IT Analytics 系统相关的信息。为确保安全无虞，管理员必须防止非管理员用户获取对这些报告的访问权限。在“**管理**”>“**用户和权限**”屏幕上设置或修改用户时，请在“**分配用户权限**”对话框中禁用“**系统控制板管理报告**”：



附录 A

常见问题解答

本附录包括下列主题：

常见问题和解决方案

问：密码如何加密以及使用哪种加密算法进行加密？

答：如果结合使用 SSO 访问门户，则用户密码存储在外部 SSO IdP 中。否则，密码将存储在 Oracle 的 AES128 加密文件中。

问：会话空闲（绝对）超时值是多少？

答：默认会话空闲超时是 15 天，但管理员可以进行自定义。

问：如何管理用户会话？

答：使用 Cookie 管理用户会话。

问：如何在平面文件中加密 Oracle 数据库密码？是否加密了任何传输中的数据？

答：如果 Oracle 和门户安装在单独的服务器上，管理员可以将该连接配置为使用 TLS 对该连接进行加密。当 Oracle 和门户安装在同一台服务器上时，不会对门户和 Oracle 之间的数据进行加密。