Delinea

Server Suite

Reporting Administrator's Guide

Version: 2023.x

Publication Date: 6/3/2024

© Delinea, 2024

Server Suite Reporting Administrator's Guide

Version: 2023.x, Publication Date: 6/3/2024

© Delinea, 2024

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

Reporting Administrator's Guide i

What Report Services Provides **1**

Reporting Data Based on Domains or Zones 2
gMSA Accounts 2
Report Services and Report Center 2
Report Services Tools Overview 2
Overview of How to Set Up Reporting 3
Evaluation Deployment Overview 4
Production Deployment Overview 5
How to Set up a Production Version of Delinea Report Services 5
Upgrade Overview 6
Using this Guide 6

Synchronized Active Directory Attributes for Reports **7**

AD Computer 7
AD Group 8
AD User 8
Application Right 9
Command Right 9
Computer Role 9
Computer SCP 10
Computer Zone AzScope 10
Computer Zone Container 10
Container 10
Desktop Right 10
Domain 11
Dzsh Command Right 11
Group SCP 11
License Container 11
Local Group SCP 12
Local User SCP 12
Network Right 12
Pam Right 13
Privileged Command Right 13
Restricted Environment 13
Role 13
Role Assignment 14
Ssh Right 14
User SCP 14
Zone 15

Installing Report Services **15**

Administering Report Services with the Report Control Panel 16

General Tab ... 16
Monitored Zones Tab ... 16
Settings Tab ... 16
Troubleshooting Tab ... 16
Before Install: Prerequisites ... 17
Supported Versions of SQL Server and SSRS ... 17
Supported Versions of PostgreSQL ... 17
Supported Browser Versions ... 17
Required User Permissions for Report Services ... 17
Report Services Account Permissions ... 18
Grant the Report Service Account Permissions ... 19
Grant the Permission to Replicate Directory Changes in ADUC ... 19
Grant the Permission To Replicate Directory Changes In ADSI ... 20
Grant the Permission to Log on as a Service ... 21
SQL Server permissions that are set by the Configuration Wizard ... 21
Sql Server Permissions Set by the Report Services Configuration Wizard (table) ... 21
PostgreSQL Permissions that are Set by the Configuration Wizard ... 23
Memory Requirements ... 23
Domain Controller Memory Requirements ... 23
Windows Memory Requirements ... 23
SQL Server Recovery Model Requirement ... 23
Impact of Using a New or Existing SQL Server Instance ... 24
Deploy in Multi-Forest Environments ... 25
Enable Selective Authentication Across a Forest with a One-Way Selective Trust ... 25
Virtual Machines and Report Services ... 25
Configuring SQL Server Reporting Services (SSRS) ... 26
Adding Your Report Services Web Site to Your Internet Explorer Trusted Sites ... 26
Granting Access in SSRS to Reports ... 28
Providing Reports to Your Users or Auditors ... 30
Sharing Reports by Email or File Sharing with Report Subscriptions ... 30
Configuring Report Services and Deploying Your Reports ... 30
Configuring a SQL Server Report Services Deployment ... 30
Configuring a PostgreSQL Report Services Deployment ... 34
Changing the Monitoring Mode for an Existing Report Services Deployment ... 38
Installing and Configuring Report Services ... 40
Re-Deploying the SQL Server Reports to SSRS ... 41
Doing a Silent Install and Configuration ... 42
Doing a Silent Install of Report Services ... 42
Configuring a New Report Services Deployment Silently ... 42
Report Services Silent Configuration Parameters ... 44
Upgrading from a Prior Version ... 48
Upgrading Your Report Services Database ... 49
Upgrading from Versions Before 2016 ... 50
Classic Zone Access Manager Reports ... 50

Hierarchical Zone Access Manager Reports 50
All Zone Access Manager Reports 51
Reports that are New to Access Manager Report Users 52
Upgrading the Reporting Database Silently 52

Building Custom Reports 53

Requirements and Recommendations 53
An Overview of Report Building Tasks 54
Migrating Custom Reports from SQL Server Express 54

Viewing Default Reports 55

Opening a Report 55
Filtering Report Data by Zone 56
Default Access Manager Reports 56
Report Services Reports: Not Specific to Classic or Hierarchical Zones 56
Delinea Report Services Reports: Classic Zone Reports 57
Delinea Report Services Reports: Hierarchical Zone Reports 58
Default SOX Attestation Reports 59
Default PCI Attestation Reports 61
How Objects are Counted for the PCI and SOX Report Charts 63
Login Report Charts 63
Login Report – By Computer charts 63
Login Report – By Group charts 64
Login Report – By Role charts 64
Login Report – By User charts 64
Login Summary Report charts 65
Rights Report Charts 65
Rights Report – By Computer Charts 65
Rights Report – By Group Charts 66
Rights Report – By Role Charts 66
Rights Report – By User Charts 66
Rights Summary Report Charts 66

Configuring Report Services for Large Active Directory Environments 67

Memory Recommendations and Requirements for Large Active Directory Environments 67
Domain Controller Memory 67
Symptoms 67
Resolution 67
Windows Memory Requirements 67
References 68
Sql Server Memory 68
Symptoms 68
Resolution 68
Configuration Recommendations for Large Active Directory Environments 68
Setting the Maximum Server Memory for SQL Server 69
Using Report Filters to Limit the Output Data of a Report 70

Symptoms ... 70
Resolution ... 70
Increasing the Time-Out Value for Rebuild/Refresh Data Operations ... 72
Symptom ... 72
Resolution ... 72
Increasing the Time-Out Values for Microsoft SQL Server Reporting Services ... 73
Report Execution Time-out ... 73
Symptoms ... 73
Resolution ... 73
HTTP Runtime Execution Timeout ... 73
Symptoms ... 73
Resolution ... 73
Increasing the ReceiveTimeOut Value for Internet Explorer ... 74
Symptoms ... 74
Resolution ... 74
Using a URL to Export Report Data to CSV ... 75
Symptoms ... 75
Resolution ... 75
References ... 75
Creating the Report Subscription for CSV Export ... 75
Prerequisites ... 76
Configuring The Report Data Source For Subscriptions ... 76
Creating A CSV Report Subscription ... 77
Skipping Chart Data From CSV Report Subscriptions ... 80

Views to Use in Custom Reports ... 81

Understanding the Differences Between Views ... 81
ADComputers View ... 83
Adcomputers Columns Used in Other Views ... 84
ADComputers_Stale View ... 84
ADGroupComputerMembers View ... 86
ADGroups View ... 87
ADGroupUserMembers View ... 89
ADUsers View ... 90
ADUser Columns Used in Other Views ... 93
ApplicationRight View ... 93
AutoZoneComputers View ... 94
CommandRight View ... 94
ComputerRoleCustomAttribute View ... 96
ComputerRoleEffectiveMembers View ... 96
ComputerRoleMembership View ... 97
ComputerRoles View ... 98
DelegationTasks View ... 99
DelegationTaskType View ... 100
Domains View ... 100

Domains Columns Used in Other Views ... 100
EffectiveAuthorizedUserPrivilegesSummary View ... 100
EffectiveAuthorizedUserPrivilegesSummary__Hierarchical View ... 101
EffectiveAuthorizedUserPrivilegesSummary_Classic View ... 101
EffectiveAuthorizedLocalUserPrivileges_Computer View ... 101
EffectiveAuthorizedLocalUsers_Computer View ... 103
EffectiveAuthorizedUserPrivileges_Computer View ... 103
EffectiveAuthorizedUsers_Computer View ... 103
EffectiveAuthorizedUsers_Computer_Classic View ... 104
EffectiveAuthorizedUsers_Computer_Hierarchical View ... 104
EffectiveAuthorizedZoneLocalUsers View ... 104
EffectiveAuthorizedZoneUsers View ... 106
EffectiveDelegationTasks View ... 107
EffectiveGroupPrivileges_Computer View ... 108
EffectiveLocalUserPrivilegesSummary View ... 110
EffectiveLocalUsersRoleAssignment View ... 110
EffectiveLoginUserPrivilege_Computer View ... 111
EffectiveRoleAssignment View ... 113
EffectiveRoleAssignment_Classic View ... 114
EffectiveRoleAssignment_Hierarchical View ... 115
EffectiveSysRights View ... 118
EffectiveUserPrivileges_Computer View ... 119
EffectiveUserPrivileges_ComputerRole_UNIX View ... 124
EffectiveUserPrivileges_ComputerRole_Windows View ... 126
EffectiveUserPrivileges_Zone_UNIX View ... 128
EffectiveUserPrivileges_Zone_Windows View ... 130
EffectiveZoneGroups View ... 132
EffectiveZoneLocalGroupMembers View ... 133
EffectiveZoneLocalGroups View ... 134
EffectiveZoneLocalUsers View ... 135
EffectiveZoneLocalWinGroupMembers View ... 136
EffectiveZoneLocalWinGroups Views ... 137
EffectiveZoneLocalWinUsers View ... 137
EffectiveZoneUsers View ... 138
RightType View ... 141
RoleAssignmentCustomAttribute View ... 142
RoleAssignments View ... 142
RoleAssignments_Computer View ... 143
RoleAssignments_ComputerRole View ... 145
RoleAssignments_Zone View ... 146
RoleCustomAttribute View ... 147
RoleRights View ... 147
Roles View ... 148
Roles Columns Used in Other Views ... 149

Roles_Classic View 149
Roles_Hierarchical View 150
TrusteeTypes View 151
Zone_Classic View 151
Zone_Hierarchical View 152
Zones_Hierarchical Columns Used in Other Views 153
ZoneComputers View 153
ZoneComputer Columns Used in Other Views 155
ZoneGroups View 155
ZoneGroup Columns Used in Other Views 156
ZoneLocalGroupMembers View 156
ZoneLocalGroups View 157
ZoneLocalUsers View 157
ZoneLocalWinGroupMembers View 158
ZoneLocalWinGroups View 159
ZoneLocalWinUsers View 159
ZoneRolePrivileges View 160
Zones View 161
ZoneUsers View 163
ZoneUser Columns Used in Other Views 165

Troubleshooting Reports 165

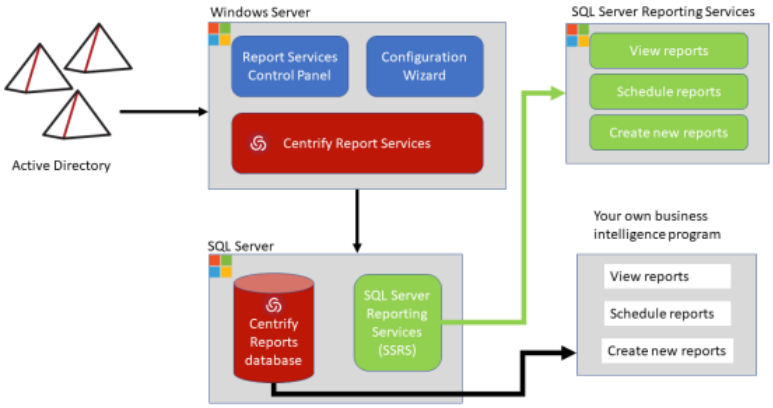
You Don't See Any data When You Open a Report 165
You Don't See the Report Builder Link in Internet Explorer 165
You Can't Log in to Report Services in Internet Explorer 165
You Get a Server Error When You Try to Synchronize with Active Directory 166
Port Conflicts 166
SSRS Fails to Start on Windows 2008 R2 Systems 167
SSRS Produces the Following Error 167
SQL Server 2008 R2 Express Edition Produces an Installation Error 167
The Report Services Configuration Wizard Cannot be Completed Due to an Error that Occurred 167
Installing SQL Server from the Delinea Management Services Installer Generates Error Codes 168
Can't install SQL Server 2012 or 2014 instance on Windows 2008 SP2 169
Report Services computation takes longer than it used to 170
Frequently asked questions about report services 170

What Report Services Provides

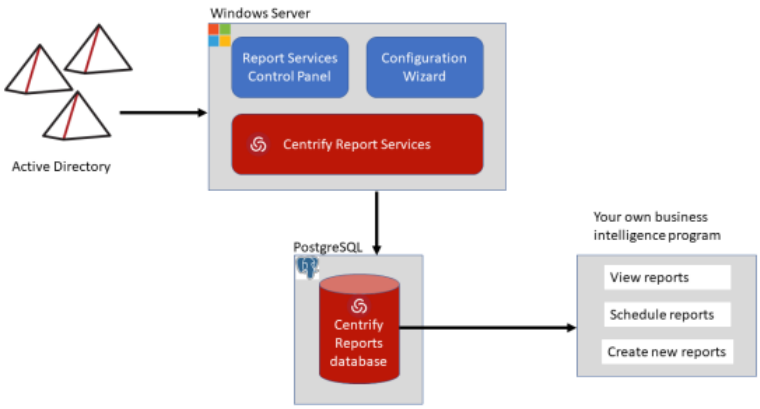
Report services provides reports on your Active Directory environment and the data is stored in a database that's optimized for reporting. You can synchronize your Active Directory information to your reporting database, and then allow your users access to the reporting data.

You can choose to use SQL Server or PostgreSQL for your report database. If you use PostgreSQL, you must provide your own report software to create and view reports.

If you're using SQL Server, the following diagram illustrates the main report services architecture components:



If you're using PostgreSQL, the following diagram illustrates the main report services architecture components:



Report services takes data from Active Directory at a particular point in time. The data collected at that point is sometimes referred to as a *snapshot*. The Active Directory data synchronization service puts the Active Directory data into tables in the reporting database, and then runs some algorithms on those tables. Some data is pulled over directly from Active Directory as it is, and some data is calculated.

For example, the effective role assignment for each computer and user is calculated rather than stored. Delinea does store the effective role assignment information at the levels of role, computer, and zone. This information is then stored in the database views, and those database views provide the information that you see in the reports.

The reporting service populates *database views* based on the data in those tables, and those views are what are used to populate reports.

Database views provide an easier and more secure way to share the reporting data without having to expose the database tables directly. Each view is essentially a database query. Some columns refer to columns in other views, and these relationships are noted.

Each default report is based on one or more of those database views, and you can build custom reports based on the information stored in one or more of those views.

For SQL Server databases, Delinea report services uses Microsoft SQL Server Reporting Services as the reporting engine for deploying and customizing reports. You can use any reporting service to generate reports by connecting to the reporting database.

Reporting Data Based on Domains or Zones

Here are some key points to be aware of if you're thinking of using report data based on zones:

- For zone-based reporting, each synchronization includes all Active Directory data from the specified zones. In comparison, for domain-based reporting, synchronizations after the first one include just the changes to Active Directory data.
- For zone-based reporting, the service account needs just read permission to Active Directory. In comparison, for domain-based reporting, the service account needs permission to replicate directory changes.
- For zone-based reporting, report services does not synchronize license information nor auto-zone computer information.
- For zone-based reporting, you can include zones from other trusted forests. For domain-based reporting, you can add trusted forest domains.

gMSA Accounts

Report services treats gMSA accounts (group Managed Service Accounts) as Active Directory users.

Information not included in the reporting database

There are few limitations on the kinds of data that can be stored in the reporting database. The following is not included:

- NIS maps
- UNIX import information

Report Services and Report Center

Report services provides more reports and features than the previous Report Center in Server Suite. Report Center has been deprecated and removed.

Report Services Tools Overview

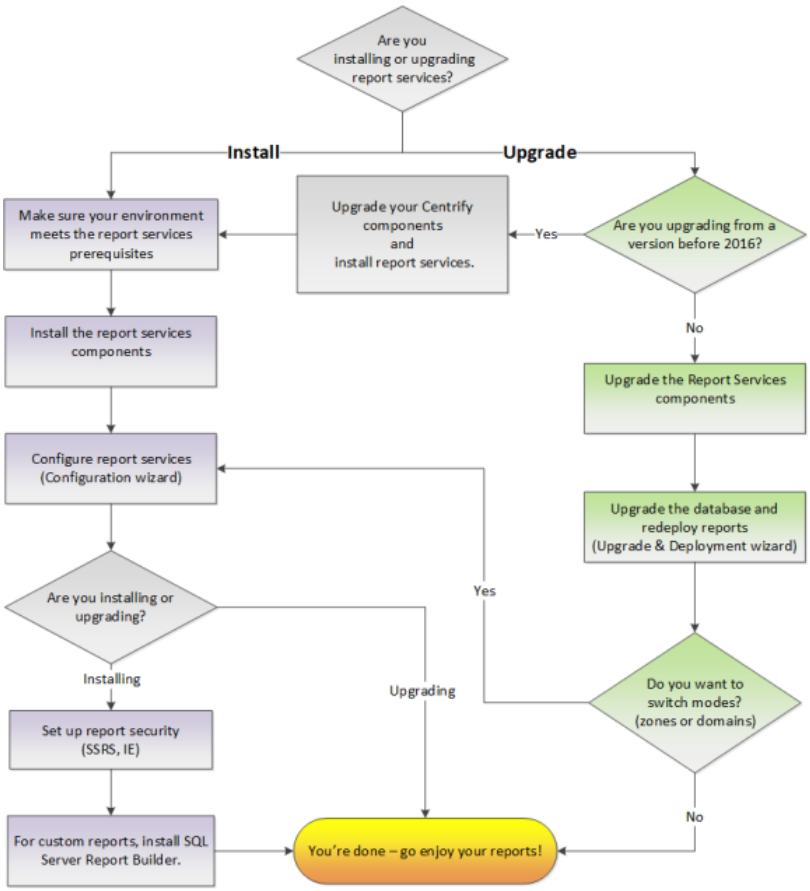
Here's an overview of the tools specific to Delinea report services. You'll use some to all of these tools, depending on whether you're completing your initial installation or changing some configuration settings later on.

Tool or component name	What you use this tool for
Report Services shortcut	Use this shortcut to open Delinea report services in Internet Explorer.
Configuration wizard	Use the configuration wizard to do the initial setup of your database and reports. Re-run the configuration wizard only if you need to change some report services configuration settings or change whether you gather report data from Active Directory based on zones or domains. For instructions, see Configuring Report Services and Deploying Your Reports .
Upgrade & Deployment wizard	Use the Upgrade & Deployment wizard to upgrade your report database and deploy updated reports. For instructions, see Upgrading your report services.
Report Services Control Panel	Use the control panel to view the synchronization status of domains or zones, refresh report data, configure the synchronization schedule, add or remove domains or zones, change the user account that runs the report service, and view error logs. For more details, see Administering Delinea Report Services with the Report Control Panel.
Server Suite installer	Use the installer to either install or upgrade the report services and other Server Suite components. For instructions, see Installing Delinea Report Rervices .

Overview of How to Set Up Reporting

If you're installing an evaluation version of Delinea report services, you can take a few shortcuts, such as using virtual machines. This section includes recommendations for both evaluation and production deployments.

The diagram below outlines the overall process for installation or upgrade.



Evaluation Deployment Overview

For evaluation purposes, you can just install the SQL Server Express version that's packaged with the Server Suite software.

How to set up an evaluation version of Delinea report services:

1. Prepare your environment:
   - Users and groups with required permissions
     a. service account - the user account that runs the reporting service (in the background)
     b. installer/administrator - the user account that installs and configures the Delinea reporting service.
     c. Report administrator - user(s) who can run reports, edit reports, build new reports
     d. Report reader - user(s) who can view reports but not edit them nor create new ones.
   - An existing database instance, if you're planning to use an existing instance.
   - The correct operating system that supports what you need. For evaluation purposes only, you can install all the software on one computer. Be sure to check that your operating system is supported for Delinea software, SQL Server, and Microsoft SQL Server Reporting Services (SSRS).

- You've configured Internet Explorer to allow access to the reporting web site. For details, see Adding Your Report Services Web Site to your Internet Explorer Trusted Sites.

2. Run the Delinea installer. Install the report services on ONE computer in your domain.
   - Do not install Delinea report services on a domain controller.
   - If you're upgrading from a prior version of Server Suite or Server Suite, the Access Manager reports are still there and they are installed anywhere you install Access Manager. In contrast, the new reporting service installs into one place in your forest. Plus, the database is optimized for reporting and retrieval.
3. Do the reporting configurations:
   - Run the Report Services Configuration wizard to configure the reporting service as needed, including starting the service.
   - Set up the report security for report administrators by assigning users and groups to SSRS roles. By default, all authenticated users have access to view reports.
   - Configure Internet Explorer.
4. View and share the reports.
5. For custom report building, make sure that you've installed Report Builder for your version of SQL Server, if you don't have it installed already. You may need to download this separately.

Production Deployment Overview

For production deployments:

- Delinea recommends that you use a production-capable version of SQL Server and not SQL Server Express.

  SQL Server Express has a limit of 10Gb of data, does not provide the ability to schedule tasks
- Delinea recommends that you do not use virtual machines.
- Use at least 4 GB memory and 2 cores. leave enough memory for the operating system and allocate the rest to SQL server. For more details, see Memory Requirements.
- Delinea recommends that you use a new database instance; do not use an existing instance of SQL server. The reason for this is because uninstalling SSRS leaves some files behind and can cause problems with re-installation, if you're reusing the database instance. For more information, see Impact of Using a New or Existing SQL Server instance.
- If you're using a PostgreSQL database, Delinea recommends using a new PostgreSQL installation.
- Do not install Delinea report services on a domain controller.

How to Set up a Production Version of Delinea Report Services

1. Prepare your environment:
   - Users and groups with required permissions. For details, see Before Installing - Prerequisites.
     a. service account - the user account that runs the reporting service (in the background)
     b. installer/administrator - the user account that installs and configures the Delinea reporting service.

c. Report administrator - user(s) who can run reports, edit reports, build new reports

d. Report reader - user(s) who can view reports but not edit them nor create new ones.

- The correct operating system that supports what you need. The operating system needs to be supported for Delinea software, SQL Server, and SQL Server Reporting Services (SSRS).

  Don't install SSRS on the domain controller.

  > Use an existing database instance with a real version of SQL Server, not the Express version. Express isn't designed to handle the performance needs of a production environment.

2. Run the Server Suite installer. Install the report services in ONE place in your forest.
   - If you're upgrading from a prior version of Server Suite, the Access Manager reports are still there and they are installed anywhere you install Access Manager. In contrast, the new reporting service installs into one place in your forest. Plus, the database is optimized for reporting and retrieval.
3. Do the reporting configurations:
   - Configure the reporting service as needed, including starting the service.
   - Set up the report security: assign users and groups to SSRS roles and configure Internet Explorer.
4. View and share the reports.
5. For custom report building, make sure that you've installed Report Builder for your version of SQL Server, if you don't have it installed already. You may need to download this separately.

Upgrade Overview

How to upgrade Delinea Report Services:

1. If you're upgrading from a version of Server Suite before version 2016, you need to install the report services components after you upgrade the other components.

   For details, see Upgrading from a Prior Version.
2. Run the installer program to upgrade your report services components.

   For details, see Upgrading from a Prior Version and the *Upgrade and Compatibility Guide*.
3. Upgrade the report database and, if you're ready to do so, redeploy your reports.

   For details, see Upgrading your Report Services Database.
4. (Optional) If you want to switch from domain-based reporting to zone-based reporting, or the other way around, run the Configuration wizard to switch modes.

   This step is optional and you can do switch modes at any time, not just during upgrade.

   For details, see Configuring Report Services and Deploying Your Reports.

Using this Guide

The guide provides the following information:

- What Report Services Provides provides an overview of the report services features and tools, including deployment overviews for production and evaluation deployments.
- Installing and Configuring Delinea Report Services provides detailed instructions for installing, upgrading, and configuring report services.
- Viewing Default Reports covers how to open a report, and provides some basic information on each of the default reports.
- Building Custom Reports provides some information about how to build your own, custom reports.
- Views to Use in Custom Reports lists the database views that you can use to populate your custom reports.
- Configuring Report Services for Large Active Directory Environments provides helpful information unique to large deployments.
- Troubleshooting Reports provides some helpful tips with common installation or configuration issues.
- Synchronized Active Directory attributes for Reports lists the object attributes that report services synchronizes from Active Directory.

Synchronized Active Directory Attributes for Reports

This section covers which Active Directory attributes that report services synchronizes for use in reports. Report services synchronizes these attributes from Active Directory to the reports database in a one-way synchronization process.

AD Computer

Active Directory class	Computer
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name sAMAccountName userAccountControl primaryGroupID dNSHostName operatingSystem operatingSystemVersion operatingSystemServicePack description whenCreated pwdLastSet objectSid sIDHistory managedBy location givenName postalAddress

AD Group

Active Directory class	group
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description gidNumber groupType mail member msSFU30GidNumber msSFU30Name msSFU30NisDomain objectSid primaryGroupToken sAMAccountName sIDHistory whenCreated managedBy

AD User

Active Directory class	user

Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name sAMAccountName userPrincipalName userAccountControl primaryGroupID msSFU30NisDomain uid uidNumber
Attributes (continued)	gidNumber loginShell unixHomeDirectory gecos msSFU30Name msSFUUidNumber msSFU30GidNumber msSFU30HomeDirectory msSFU30Gecos whenCreated
Attributes (continued)	lastLogonTimestamp accountExpires lockoutTime pwdLastSet givenName sn initials displayName description
Attributes (continued)	physicalDeliveryOfficeName telephoneNumber mail wWWHomePage objectSid SIDHistory streetAddress postOfficeBox l st
Attributes (continued)	postalCode co homePhone otherHomePhone pager otherPager mobile otherMobile facsimileTelephoneNumber otherFacsimileTelephoneNumber

Attributes (continued)	ipPhone otherIpPhone title department company manager profilePath scriptPath homeDirectory homeDrive msNPAllowDialin
Attributes (continued)	msNPCallingStationID msRADIUSServiceType msRADIUSCallbackNumber msRADIUSFramedIPAddress msRADIUSFramedRoute

Application Right

Active Directory	msDS-AzOperation
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-AzOperationID

Command Right

Active Directory class	msDS-AzOperation
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-AzOperationID

Computer Role

Active Directory class	msDS-AzScope
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-AzOperationID

Computer SCP

Active Directory class	serviceConnectionPoint
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName keywords managedBy whenCreated

Computer Zone AzScope

Active Directory class	msDS-AzScope
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName msDS-AzScopeName

Computer Zone Container

Active Directory class	container
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName description

Container

Active Directory class	all possible container classes
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name

Desktop Right

Active Directory class	msDS-AzOperation

Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-AzOperationID

Domain

Active Directory class	domainDNS
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	msDS-LogonTimeSyncInterval distinguishedName lockoutDuration

Dzsh Command Right

Active Directory class	msDS-AzOperation
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-AzOperationID

Group SCP

Active Directory class	serviceConnectionPoint
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName keywords gidNumber managedBy

License Container

Active Directory class	classStore

Available in zone mode?	No
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName description whenCreated

Local Group SCP

Active Directory class	serviceConnectionPoint
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName keywords gidNumber

Local User SCP

Active Directory class	serviceConnectionPoint
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName keywords uid uidNumber gidNumber unixHomeDirectory loginShell gecos

Network Right

Active Directory class	msDS-AzOperation
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-AzOperationID

Pam Right

Active Directory class	msDS-AzOperation
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData

Privileged Command Right

Active Directory class	msDS-AzOperation
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-AzOperationID

Restricted Environment

Active Directory class	msDS-AzTask
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-OperationsForAzTask

Role

Active Directory class	msDS-AzTask
Available in zone mode?	Yes

Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData msDS-OperationsForAzTask msDS-TasksForAzTask

Role Assignment

Active Directory class	msDS-AzRole
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName msDS-AzApplicationData msDS-TasksForAzRole msDS-MembersForAzRole

Ssh Right

Active Directory class	msDS-AzOperation
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description msDS-AzApplicationData

User SCP

Active Directory class	serviceConnectionPoint
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name displayName name keywords uid uidNumber gidNumber unixHomeDirectory loginShell gecos managedBy

Zone

Active Directory class	container or OU
Available in zone mode?	Yes
Available in domain mode?	Yes
Attributes	objectGUID parentGUID name description displayName

Installing Report Services

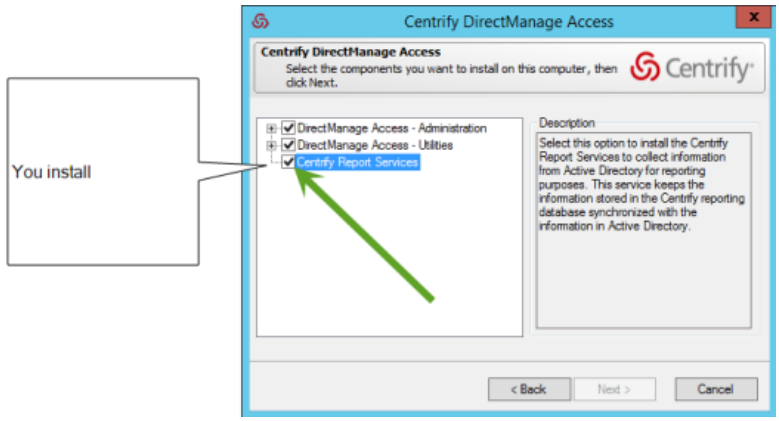
You use the same installer to install report services that you use to install other Server Suite components.

To install Delinea Report services:

1. Run the Delinea Management Services installer program that's appropriate for your Windows system (64-bit only).
2. In the Getting Started screen, click **Access**.
3. In the Welcome screen, click **Next** to continue.
4. Review the license agreement, and click the option that indicates that you agree to the terms.

   Click **Next** to continue.
5. In the User Registration screen, enter your name and company name.

   Click **Next** to continue.
6. Select the **Centrify Report Services** item.



   You can install other Server Suite components at this time, or install the other components later.

   Click **Next** to continue.
7. In the Choose Destination Folder screen, specify the folder you want to install the software.

If you're also installing Access Manager, you can select the options to automatically install desktop shortcuts.

Click **Next** to continue.

In the Confirm Installation Settings screen, review the list of components that will be installed. If the list is correct, click **Next** to continue.

The program installs the files.

8. In the completion screen, select **Configure Report Services** and click **Finish**. Proceed to the next section, Configuring report services and deploying your reports .
9. If you don't want to configure report services right now, deselect the **Configure Report Services** option and click **Finish**. You can run the configuration wizard later, if desired.

Administering Report Services with the Report Control Panel

You can use the Delinea Report Services Control Panel for the following tasks:

General Tab

- View the status of data synchronization from Active Directory to the report database
- View the domains or zones that are included for reporting
- Start, stop, or restart the reporting service.

Monitored Zones Tab

This tab appears only if you've configured reporting based on specific zones instead of domains.

- Edit the Hierarchical or Classic zones that you want to include in your reports. You can add or remove zones, as desired, and you can select zones from other trusted forests.

Settings Tab

- Configure when the reporting service synchronizes data from Active Directory to the reporting database
- Change the user account that runs the reporting service.
- Add, edit, or remove domain controllers (in zone-based monitor mode) or domains (in domain-based monitor mode).
- If you're using a PostgreSQL database, you can test the connection to the database.

Troubleshooting Tab

- View the log files and set the level of detail that are collected in the log files.
- Export diagnostics data for use by Delinea Technical Support (if technical support requests that you do so).
- Rebuild or refresh the reports data
- Validate that the reporting service has the correct permissions to read data from the monitored domains and replicate the data.

Before Install: Prerequisites

For the full set of platform requirements, please visit this web page in the Delinea Technical Support area:

https://www.centrify.com/support/whats-new/infrastructure-services/

Supported Versions of SQL Server and SSRS

To use Delinea report services, you need to use a SQL Server that is one of the following versions:

- SQL Server 2008 R2
- SQL Server 2012
- SQL Server 2012 R2
- SQL Server 2014
- SQL Server 2016
- SQL Server 2019

For Microsoft SSRS, use the version that correlates with your SQL Server version. For example, if you're using SQL Server 2012 R2, then use Microsoft SSRS version 2012 R2.

If you choose to use a version of SQL Server that requires .NET version 3.5 SP1, be sure to install .NET before configuring report services.

If you run Report Services with Microsoft SQL Server 2012 Service Pack 2 and Visual Studio 2010 on the same system, please update Visual Studio 2010 to Service Pack 1. (Ref: CS-38553a)

Supported Versions of PostgreSQL

Delinea Report Services works with PostgreSQL databases that are version 11 or later.

Supported Browser Versions

Use the web browser versions that Microsoft supports for use with SQL Server Reporting Services, as mentioned in this page:

https://msdn.microsoft.com/en-us/library/ms156511.aspx

For Internet Explorer, the version of SQL Server and SQL Server Reporting Services (SSRS) that you use also determines which version of Internet Explorer is compatible with your deployment. Please consult the Delinea Knowledge Base article KB-6671 for details about which version of Internet Explorer you should use.

Required User Permissions for Report Services

Before you install Delinea report services, be sure you have the appropriate software and user accounts, which includes the following:

- Users with required permissions. Before installation, you must have users to run the Delinea installer.
- Report service account
- SQL Server service account (this is needed if you're installing using an existing instance)
- User accounts that can run the Report Configuration Wizard and the Reporting Control Panel.

  There are a few user accounts that you need to set up for use with Delinea report services. Here is a summary of the user accounts that you need to create and the permissions you need to explicitly grant.

Report Services Account Permissions

User type	Required Active Directory permissions	Required security policy permissions (group policy, or local policy)	Required SSRS permissions	Required SQL Server or PostgreSQL permissions
report service account to run the Reporting Service	For domain-based reporting: Replicating directory changes at the domain level (ADUC) and replicate directory changes in ADSI For zone-based reporting: Read permission	Log on as a service		
SQL Server service account to run SQL Server	n/a	Log on as a service		member of the securityadmin role
PostgreSQL service account				the account must have permission to connect to PostgreSQL and create a database
report admin to run the Report Configuration wizard or the Upgrade & Deployment wizard and deploy reports to an existing SQL Server instance	needs to be a member of the domain	n/a	Folder Settings > Content Manager role	member of the securityadmin role (At the very least, the user needs permission to connect to SQL Server and create a database.)

report admin to modify the Reports Control Panel	Read permission to the domain root object of the selected domain. Read permission to all computer objects in the selected domain.	n/a		
Report viewer to view reports from SSRS/Internet Explorer			Site settings > System user role Folder settings > browser (assign SSRS roles to Active Directory group or users)	
Report writer read, write, edit access for reports, in addition to the permissions needed to view reports			Site settings > System user role Folder settings > Content Manager role (assign SSRS roles to Active Directory group or users)	

Delinea Report Services requires administrator permission to install and upgrade. That also means that only an administrator can uninstall and repair Delinea Report Services. (Ref: CS-40808a)

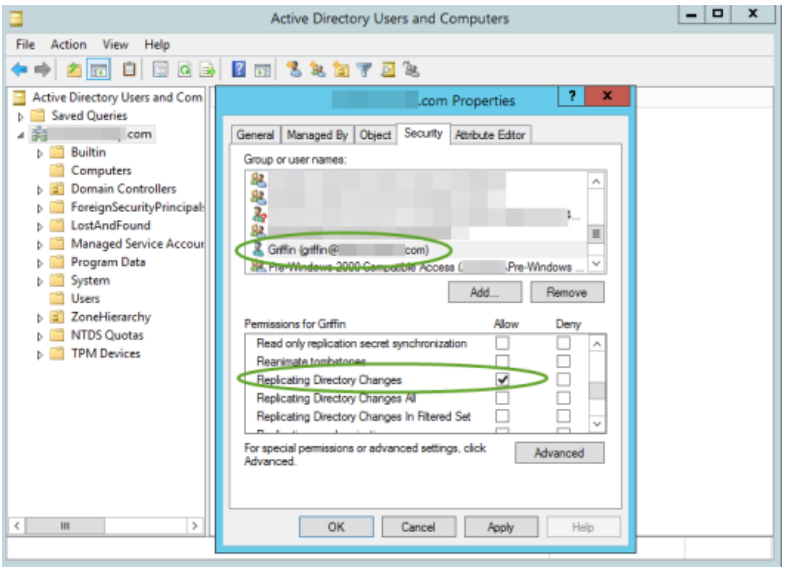
Grant the Report Service Account Permissions

For your convenience, below are reminders for how to grant the two sets of required permissions for the report service account.

Grant the Permission to Replicate Directory Changes in ADUC

To grant the permission to replicate directory changes at the domain level (read only):

1. Open Active Directory Users and Computers.
2. From the View menu, select **Advanced Features**.
3. Right-click the domain object and select **Properties**.
4. Click the **Security** tab.
5. Select the desired user account (add the account if it's not listed there already).
6. In the Permissions area, next to **Replicating Directory Changes**, click **Allow**.



7. Click OK to save your changes.

   For more information about setting this permission, see https://support.microsoft.com/en-us/kb/303972.

Grant the Permission To Replicate Directory Changes In ADSI

In addition to granting the replicate directory changes permission in Active Directory Users and Computers (ADUC), you also need to grant the same permission in the ADSI Edit (Active Directory Services Interfaces Editor) console.

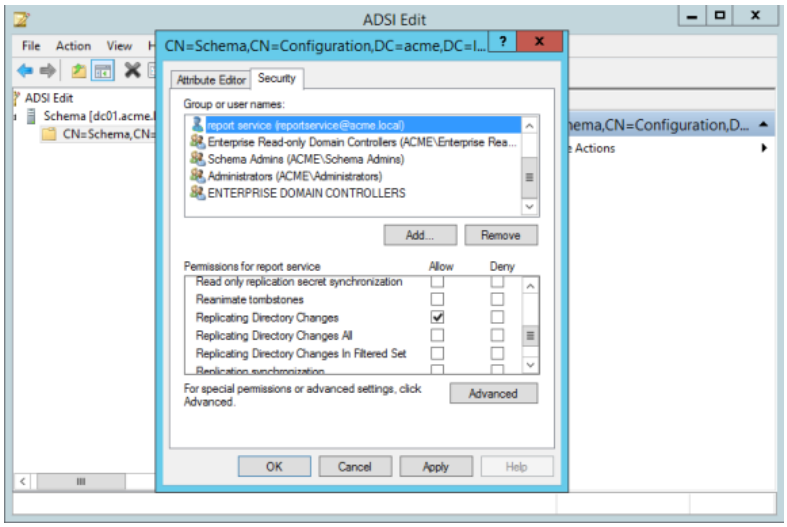
To grant the permission to replicate directory changes in ADSI (read only):

1. Open the ADSI Edit console.
2. From the Action menu, select **Connect to**.

   The Connection Settings dialog box opens.
3. For the Connection Point, go to the "Select a well known Naming Context" drop-down menu and select **Schema**.
4. Click **OK** to close the dialog box.

   The schema for the current domain displays in the ADSI Edit console.
5. Expand the schema listing so that you can see the first node of the schema, and right-click that node and select **Properties**.

   The Attribute Editor dialog box opens.
6. Click the **Security** tab.
7. Select the desired user account (add the account if it's not listed there already).
8. In the Permissions area, next to **Replicating Directory Changes**, click **Allow**.



9. Click OK to save your changes.

Grant the Permission to Log on as a Service

To grant the log on as a service permission:

1. In the Group Policy Management Editor, apply the following policy to your desired user or group of users:

   Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Log on as a Service.

For more details about granting the log on as a service policy, see https://technet.microsoft.com/en-us/library/dn221981(v=ws.11).aspx.

SQL Server permissions that are set by the Configuration Wizard

Here are the SQL server permissions that report services grants to each user type, for your information. The Report Services Configuration wizard sets these permissions automatically.

Sql Server Permissions Set by the Report Services Configuration Wizard (table)

User type	Required SQL Server permissions
report services account to run the SQL Server Reporting Service	Snapshot Service (predefined role)

SQL Server service account to run SQL Server	If you deploy to an existing SQL Server instance, the configuration wizard makes no changes to the SQL Server service account. If you deploy to a new SQL Server instance: --If the operating system is Windows 2008 and you're using a SQL Server version later than 2012, virtual accounts are used for various SQL Server components, as follows: SQL Server engine: NT SERVICE\MSSQL$<InstanceName> SQL Server Agent: NT SERVICE\SQLAgent$<InstanceName> Full text search: NT SERVICE\MSSQLFDLauncher$<InstanceName> SSRS: NT SERVICE\ReportServer$<InstanceName> --Otherwise, the SQL Server service accounts are configured as follows: SQL Server engine: NT Authority\Network Service SQL Server Agent: NT Authority\Network Service Full text search: NT Authority\Local Service SSRS: NT Authority\Local Service
report admin to run the Report Configuration Wizard and deploy reports to an existing SQL Server instance	Connect SQL (cannot be revoked after setup) Create Database, Create any database, or Alter any database member of securityadmin role, or Alter any login permission
report admin to modify the Reports Control Panel	SnapshotAdmin (predefined role)
Report viewer to view reports from SSRS/Internet Explorer	Login permission SnapshotViewer (predefined role)
Report writer read, write, edit access for reports, in addition to the permissions needed to view reports	Login permission SnapshotViewer (predefined role)

Microsoft SQL Server Reporting System (SSRS) affords only role-based security in their reports. Be sure to grant appropriate access to reports. For example, if a user has access to only some data in the specified domain but all reports, they will be able to view all reports on all data from Active Directory.

PostgreSQL Permissions that are Set by the Configuration Wizard

When you create the PostgreSQL database with the Configuration wizard, the wizard grants the administrator user one permission for Create Database.

Memory Requirements

Be sure that your computers running the following components meet or exceed the RAM requirements listed below.

Domain Controller Memory Requirements

The minimum amount of RAM that you should have available for your domain controller is the sum of the following:

- Active Directory database size (for example, C:\Windows\NTDS\)
- Total SYSVOL size (for example, C:\Windows\SYSVOL)
- Recommended amount of RAM for your operating system
- Vendor recommended amount of RAM for your various background software agents, such as anti-virus, monitoring, backup, and so forth.
- Additional RAM to accommodate growth over the lifetime of the server.

For more information, see Microsoft recommendations here: http://social.technet.microsoft.com/wiki/contents/articles/14355.capacity-planning-for-active-directory-domain-services.aspx.

Windows Memory Requirements

Here are the minimum and recommended memory requirements for report services and the report database:

- Delinea report services: minimum 2 GB RAM, recommended 4 GB or above
- SQL Server report database: minimum 4 GB RAM, recommended 32 GB or above
- PostgreSQL report database: minimum 4 GB RAM, recommended 32 GB or above

SQL Server Recovery Model Requirement

In order for report services to function efficiently, it's recommended that you configure your SQL Server database to use the Simple recovery model. The recovery model configuration determines how SQL Server logs transactions, whether a database backs up the transaction log, and what kinds of restore options are available.

For more information about recovery models, please visit https://msdn.microsoft.com/en-us/library/ms189275.aspx.

To configure the SQL Server database recovery model:

1. In SQL Server Management Studio, navigate to the database that you use for report services.
2. Right-click the database and select **Properties**.
3. In the Select a Page area, click **Options**.

4. For the Recovery Model option, select **Simple**.
5. Click **OK** to save the changes.

Impact of Using a New or Existing SQL Server Instance

When you set up your installation of Delinea report services, you have the option of either using an existing SQL Server instance or installing a new instance. Delinea recommends that you use a new SQL Server instance, if possible.

If you choose to install a new instance from the Delinea Management Services installer program, the program installs an instance of SQL Server Express 2008 R2 with Advanced Services.

If you have an existing installation of SQL Server, you can create a new instance there first on your own, using your own installation media. When you install or configure Delinea report services, you then configure report services to use your existing instance that you created. That way, your SQL Server instances use the same edition and version.

Tip: Please see the information at the following link for details about installing multiple versions and instances of SQL Server:

https://msdn.microsoft.com/en-us/library/ms143694(v=sql.130).aspx

Here are some issues to be aware of if you're going to use a *new* SQL Server instance:

- With a new SQL Server instance, you can avoid any potential problematic issues with SSRS, particularly if you need to reinstall SSRS.
- SSRS won't slow down the regular database operations on other instances.
- To prevent the SQL Server instance from consuming too much memory, it's recommended to use the max server memory to control each SQL Server instance's memory usage. The total allowance is not more than the total physical memory on the machine. If user is not running all of the instances, none of the running instances will be able to utilize the remaining free memory.

Here are some issues to be aware of if you're going to use an *existing* SQL Server instance:

- There can be issues with SSRS and existing instances. If you have to uninstall and reinstall SSRS, it leaves files behind with the existing instance.
- Using an existing SQL server instance can use all the free memory with a larger limit of the max server memory setting.

If you choose to deploy report services using an existing instance of SQL Server, your database administrator may need to know what changes that report services needs to make to the database. (KB-8042)

The only modification that report services makes to an existing database instance is to add two Windows integrated logins, as follows:

Login	Granted database role for the Report Service database
<The specified service account>	SnapshotService

[NT Authority\Authenticated Users]	SnapshotViewer

If these logins already exist, report services does not re-create them.

Deploy in Multi-Forest Environments

If you're deploying report services across multiple forests, there are a few tips to be aware of.

- It is best to install report services once in a forest, and then monitor domains or zones in other trusted forests.
- If you use domain-based mode, you need to install report services once in the domain. Make sure that any users who run report services and the service account have access to the domains for which you want to run reports.

If you need to grant access to a user account across a forest with a one-way selective trust, you enable selective authentication for that user.

Enable Selective Authentication Across a Forest with a One-Way Selective Trust

The instructions below are provided as a courtesy; for more information on selective authentication, see the following article:

https://technet.microsoft.com/en-us/library/cc794747(v=ws.10).aspx

How to enable selective authentication for a user across an Active Directory forest that has a one-way selective trust:

1. Open **Active Directory Domains and Trusts.**
2. In the console tree, right-click the domain node for the forest root domain, and then click **Properties**.
3. On the **Trusts** tab, under either **Domains trusted by this domain** (outgoing trusts) or **Domains that trust this domain** (incoming trusts), click the forest trust that you want to administer, and then click **Properties**.
4. On the **Authentication** tab, click **Selective authentication**, and then click **OK**.
5. Open **Active Directory Users and Computers**.
6. Navigate to the Domain Controller the Report Services will use, right-click the computer object, and then click **Properties**.
7. On the Security tab add the desired user and grant Allow for the **Allowed to authenticate** permission.

See also the Delinea knowledge base article KB-8071.

Virtual Machines and Report Services

For production deployments, it is recommended to avoid using virtual machines for use with report services. (KB-7038)

In general, report services works well in virtual machines, including the case of installing SQL Server in a virtual machine.

However, in a large enterprise environment (such as where more than 100,000 users are enabled for authentication service), the SQL queries used for generating reports may have significant CPU, memory and I/O requirements. In

these situations, Delinea recommends the use of physical computers for SQL Server to allow for better tuning of SQL Server without impacting other systems.

Alternatively, you can install SQL Server in a virtual machine. In such cases, Delinea recommends that you follow the guidelines provided by the virtualization vendors:

https://www.vmware.com/files/pdf/solutions/SQL_Server_on_VMware-Best_Practices_Guide.pdf

http://download.microsoft.com/download/6/1/d/61dde9b6-ab46-48ca-8380-d7714c9cb1ab/best_practices_for_virtualizing_and_managing_sql_server_2012.pdf

Configuring SQL Server Reporting Services (SSRS)

This section includes the following topics:

- Adding your report services web site to your Internet Explorer trusted sites
- Granting access in SSRS to reports
- Providing reports to your users or auditors
- Sharing reports by email or file sharing with report subscriptions

Adding Your Report Services Web Site to Your Internet Explorer Trusted Sites

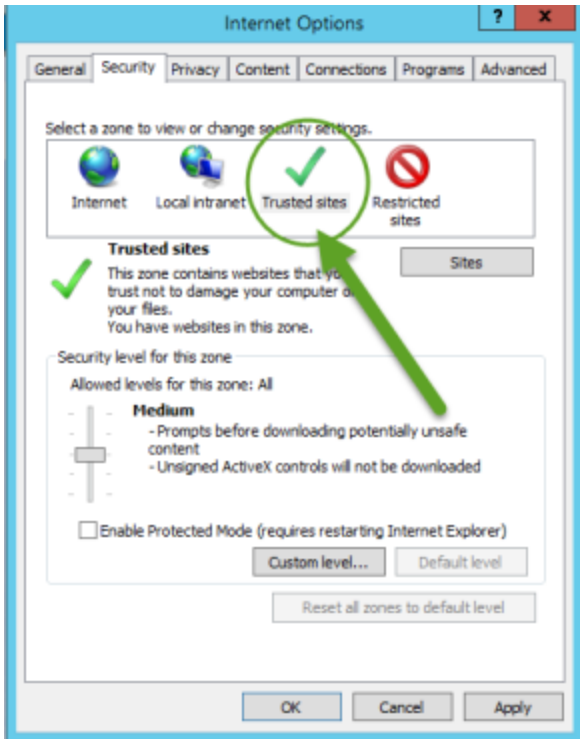
Chrome, Firefox, and Safari are NOT supported for SSRS. This is a Microsoft limitation.

In order to view the reports in Internet Explorer, you also have to add the report server as a trusted site. (If you're running an evaluation version, you can also choose to disable the Internet Enhanced Security configuration, but it's not recommended to do so.)

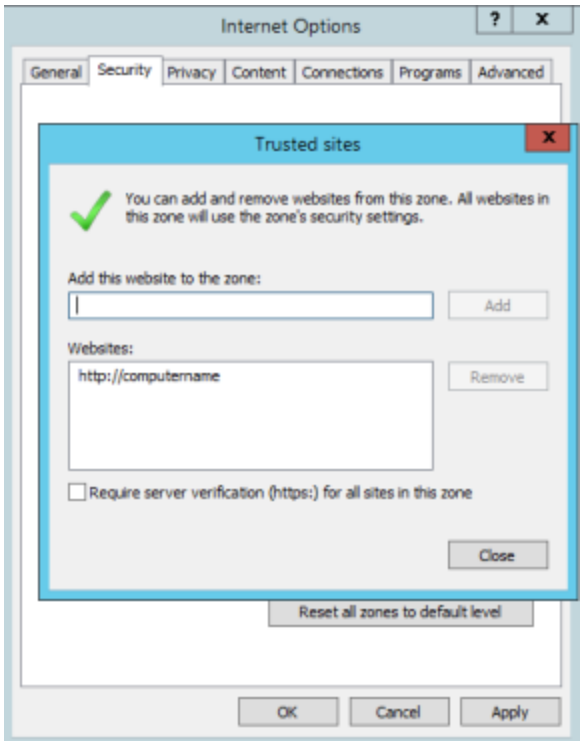
Please consult Microsoft documentation for the most current instructions for Internet Explorer configuration. However, for your convenience, here's a quick reminder of how to add a trusted site.

To configure Internet Explorer to trust the report services deployment site in the local intranet zone:

1. In Internet Explorer, go to **Tools** > **Internet Options**.
2. Click **Security**.
3. In the Zones area, click **Trusted Sites**.



4. Click **Sites**.
5. In the Trusted Sites dialog box, enter the web site address for your report services deployment, and click **Add**.



For example, enter a URL that looks something like this: http://computername/reportinstancename.

6. Click **Close**, and then click **OK** to save the changes.

Granting Access in SSRS to Reports

Before you provide reports to your users, you need to give them the appropriate access within the Microsoft SQL Server Reporting Services application. You use the SSRS role-based security to assign Active Directory users and groups to SSRS roles for both the site and folders.

Anyone reading reports will also need to configure their Internet Explorer installation, as mentioned in Adding your report services web site to your Internet Explorer trusted sites.

Please consult Microsoft documentation for the most current instructions for security configuration and granting access in SSRS. For example, some information can be found at this link:

https://docs.microsoft.com/en-us/sql/reporting-services/report-server/configure-a-native-mode-report-server-for-local-administration-ssrs?view=sql-server-2016

However, for your convenience, a couple procedures are below.

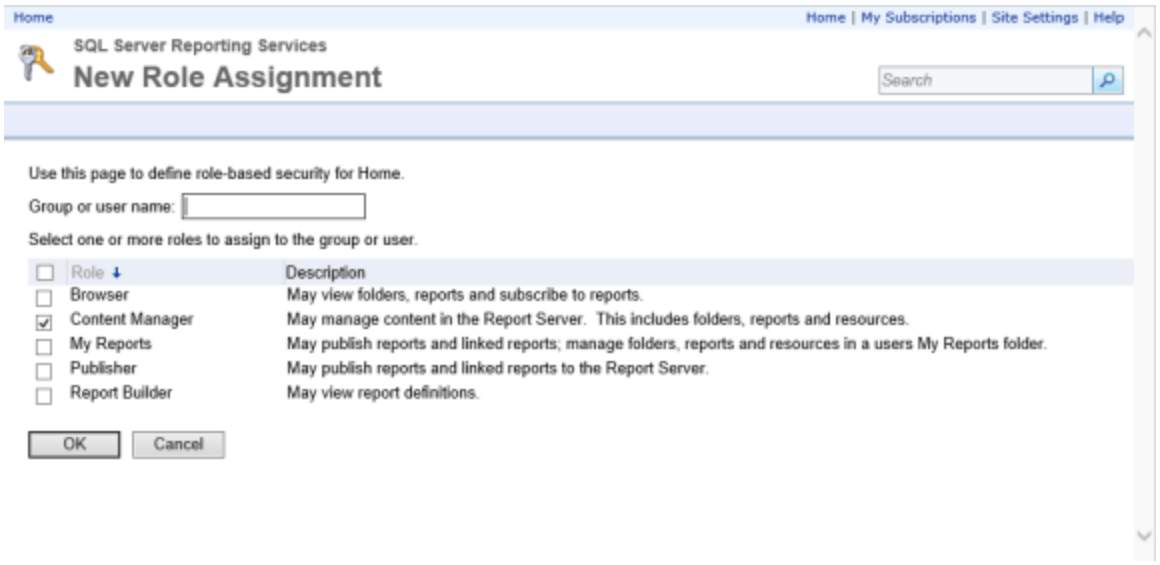
To grant report **administrator** access in SSRS (SQL Server Reporting Services):

1. Run Internet Explorer as Administrator.
2. In Internet Explorer, go to your Report Manager URL.

   You can open the Microsoft Reporting Services Configuration Manager to view the Report Manager URL.

   Internet Explorer opens SQL Server Reporting Servies to your Report Manager URL.
3. Click **Site Settings**, and create a new role assignment so that you can assign the desired Active Directory group to the “System Administrator” role in SSRS.

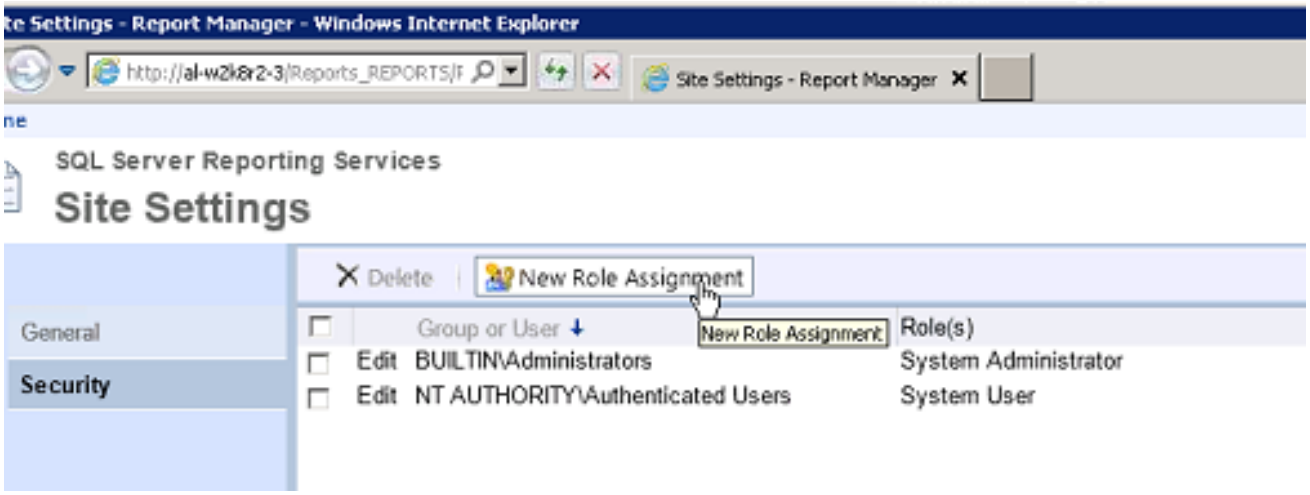
   To create a new role assignment, click **Security**, then **New Role Assignment**.
4. Enter the group or user name (in the domain\username formet), select **System Administrator**, and click **OK**.
5. Click **Home**, and then click **Folder settings**. From there, create a new role assignment so that you can grant access to the “Content Manager” role.



6. To grant access so that the user can **edit or build** reports, you can give them additional permissions in SSRS, such as the Report Builder permission to the Home folder.

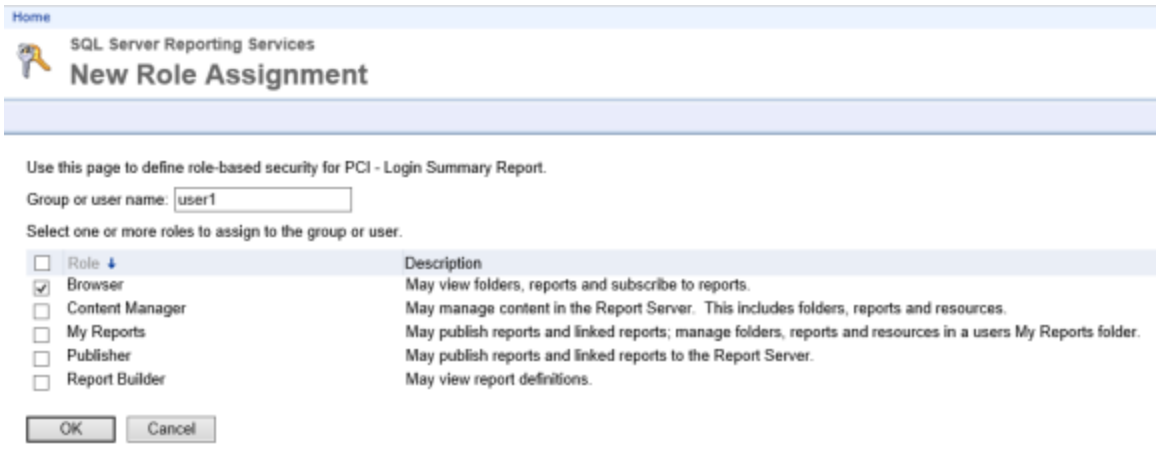
To grant report **read** access in SSRS (an overview):

1. In SSRS, go to Site Settings, and create a new role assignment so that you can assign the desired Active Directory group to the “System user” role in SSRS.



   By default, all authenticated users are assigned to the System User role.

2. In SSRS, go to the Home folder, and then click Folder settings. From there, create a new role assignment so that you can grant access to at least the “Browser” role.



3. To grant access so that the user can **edit or build** reports, you can give them additional permissions in SSRS, such as the Report Builder permission to the Home folder.

Providing Reports to Your Users or Auditors

After you've made sure that your users have the appropriate read access to reports within SSRS, you provide the report URL to your users and instruct them to access that URL within your domain and using the Internet Explorer browser. They may also need to add the report URLs to their trusted domains list; for details, see Adding your report services web site to your Internet Explorer trusted sites.

Sharing Reports by Email or File Sharing with Report Subscriptions

You can also create report subscriptions so that you can easily share reports by way of email or a file share. These are features of Microsoft SSRS, and the Microsoft documentation has the latest information.

In order to share reports by email, you first need to configure your report server for email delivery. For details, see https://msdn.microsoft.com/en-us/library/ms345234(v=sql.110).aspx.

For details for how to share reports by email or file sharing, see https://msdn.microsoft.com/en-us/library/ms189680(v=sql.110).aspx.

Configuring Report Services and Deploying Your Reports

You use the configuration wizard to both set up a new report services deployment or reconfigure an existing one.

If you want to just redeploy your reports, see Re-deploying SQL Server reports to SSRS.

Configuring a SQL Server Report Services Deployment

Follow these instructions if you're creating a new report services deployment using SQL Server or reconfiguring an existing SQL Server report services deployment.

To configure report services with a SQL Server database:

1. If you need to start the Delinea Report Services configuration wizard, go to the **Start** menu > **All Programs** > **Centrify Server Suite 2021.1** > **Report Services**, and choose **Configuration Wizard.**

   If you're continuing from the Delinea Management Services installer, the installer started the configuration wizard for you.

2. On the Welcome screen, click **Next** to continue.
3. If you have already set up report services, the Reconfiguring Report Services screen displays. Select **Reconfigure** and click **Next** to continue.
4. On the Database Type screen, select **SQL Server** and click **Next** to continue.
5. Configure the SQL Server database connection:
   a. Specify the SQL Server instance name.

      Either specify a new SQL Server instance name, or select an existing SQL Server instance name. (The default instance name is CENTRIFYSUITE.)

      The SQL Server instance name must be 16 characters or less, the name cannot begin with an underscore (_) or dollar sign ($), and the instance name cannot contain any of the following special characters: a blank space, backslash (\), comma (,), colon (:), semi-colon (;), single quotation mark ('), ampersand (&), hyphen (-), number sign (#), or at sign (@).

      If you select an existing SQL Server instance, be aware that the SQL Server browser service must be running if SQL Server is a named instance or using dynamic ports. If for some reason the SQL Server service can't be started, you need to provide the SQL Server instance name and port number in order to connect to the database successfully. For additional details, see https://technet.microsoft.com/en-us/library/ms181087(v=sql.105).aspx.

      Delinea recommends that you use a new SQL Server instance, if possible. For more information, see Impact of using a new or existing SQL Server instance.

   b. The default database name is *Report*. You can change this, if desired.

      The SQL Server database name must be 16 characters or less, the name cannot contain any of the following special characters: backslash (\), forward slash (/), colon (:), asterisk (*), question mark (?), double quotes (“), less-than sign (<), greater-than sign (>), pipe (|), comma (,) or single quotation mark (').

   c. Click **Next** to continue.
   d. If you selected to install a new SQL Server instance, click **Browse** to navigate to and specify the location of the SQL server installation executable (*.exe file).

      The installer program installs SQL Server 2008 R2 Express with Advanced Services.

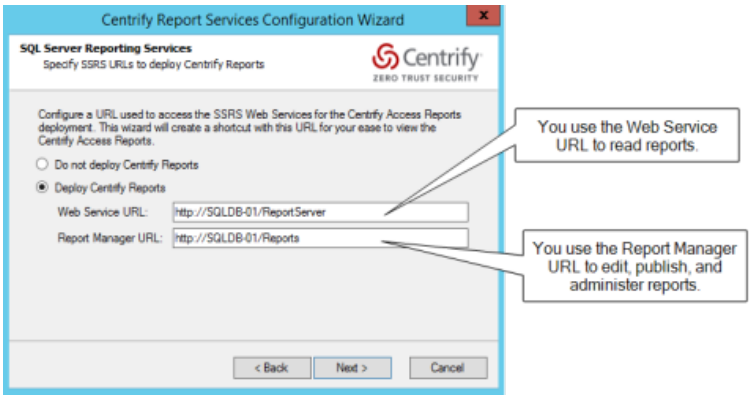
      You can download the SQL Server Express with Advanced Services package directly from Delinea, for your convenience. Or, download the package from Microsoft.

      Please ensure to download the file name SQLEXPRADV_x64_ENU.exe (1,008.6 MB in size) as this is the one containing the 64-bit edition of SQL 2008 R2 with the necessary additional components to support Delinea Reporting Services.

   e. Click **Next** to continue.
6. Deploy the reports:

a. In the SQL Server Reporting Services screen, specify whether to deploy the Server Suite reports (or not).

If you plan to use a reporting solution other than Microsoft SQL Server Reporting Services, do not deploy the reports.



This screen also lists the URLs for the Reporting Web Service and Report Manager. You'll use these URLs later to access to the reports.

If you're using a production server of SQL Server and SSRS, you can configure them to use HTTPS. For details, see Microsoft SQL Server and SSRS documentation, such as https://msdn.microsoft.com/en-us/library/ms345223.aspx.

The configuration wizard populates the report URLs automatically. If you had specified to use an existing SQL Server instance, the configuration wizard retrieves the existing web service URL and report manager URL for your SQL Server instance.

For an existing SQL Server instance, you can open the Microsoft Reporting Services Configuration Manager to view the Web Service and Report Manager URLs.

b. Click **Next** to continue.

7. Choose domain or zone reporting:

Specify whether you want to choose data for reporting based on domains or zones. The default is domain-based reporting.

Click **Next** to continue. If you selected domain-based reporting, proceed to the next step. For zone-based reporting, go to Step 8.

8. If you selected domain-based reporting:

a. In the Monitored Domain(s) screen, you can review and edit the list of domains that will be included for reporting. Add or remove domains as desired.

For each domain, the configuration wizard lists the domain name and the domain controller name.

b. Click **Next** to continue.

9. If you selected zone-based reporting and you use hierarchical zones:

a. If you want data from all zones, select **Monitor all hierarchical zones from forest(s)**. You can add or edit forests by clicking **Edit** and then adding or removing forests.

b. Or, if you want to report data from specific zones, select **Monitor only specific hierarchical zones**.

c. Click **Edit**.

   The Specify Forest for zone selection dialog box opens.

d. Enter the forest name where the desired zones are and click **OK**.

   The Edit Monitored Hierarchical Zones dialog box opens.

e. Enter the hierarchical zones by name, or expand the list of zones to locate the desired zones manually.

f. If desired, specify to select the parent or child zones automatically.

g. Select the zone by putting a checkmark in the box next to the zone name.

h. When you're done specifying which hierarchical zones to monitor, click **OK** to close the dialog box and return to the Configuration wizard.

   Each zone that you've selected is listed in the Hierarchical Zones screen.

i. Click **Next** to continue.

10. If you selected zone-based reporting and you use classic zones:

    a. If you want data from all zones, select **Monitor all classic zones from forest(s)**. You can add or edit forests by clicking **Edit** and then adding or removing forests.

    b. Or, if you want to report data from specific zones, select **Monitor only specific classic zones**.

    c. Click **Edit**.

       The Specify Forest for zone selection dialog box opens.

    d. Enter the forest name where the desired zones are and click **OK**.

       The Edit Monitored Classic Zones dialog box opens.

    e. Select the classic zones to include in your reports. Select the zone by putting a checkmark in the box next to the zone name.

       You can filter the list of zones by entering a portion of the name and clicking **Filter**.

    f. When you're done specifying which classic zones to monitor, click **OK** to close the dialog box and return to the wizard. Click **Next** to continue.

11. For zone-based reporting, you can also specify which domain controller(s) that the report service connects to.

    If you don't specify which domain controller(s) to use, report services will use the default domain controller.

    a. Click **Add**.

       The Add Domain Controller dialog box opens.

    b. Enter the domain name and then select the domain controller from the list.

    c. Click **OK** to return to the Configuration wizard.

The domain controllers that you selected are listed in the wizard screen.

d. Click **Next** to continue.

12. In the Synchronization schedule screen, specify how often you want the reporting service to pull data from Active Directory.

    You can specify that the service synchronizes weekly, daily, every certain number of days, or every certain number of hours. The limit is 32,767 days or weeks.

    Click **Next** to continue.

13. Configure the user account that runs the service:

    a. In the Report Services options screen, specify the user account that will be used to run the service that synchronizes data from Active Directory and the reporting database.

       You can select a network service account, a managed service account, or another user account in Active Directory.

       You must specify a user account that has the required permissions. The configuration wizard verifies that the user has the correct level of access.

    b. Click **Next** to continue.

    c. The configuration wizard verifies that the specified user account has the required permission. An error displays if the permissions are inadequate.

    d. If the permission verification is successful, click **Close** to close the Verify permission window.

14. Review and complete the installation:

    a. In the Summary screen, review the installation details. If the installation settings are correct, click **Next** to continue.

       If you're installing a new database, it may take a few minutes.

    b. (Optional) In the completion screen, if the installation is successful, you can select the option to synchronize Active Directory data with the report database immediately. Depending on the Active Directory configuration and domain size, this operation can take awhile to complete.

       Or, alternatively, you can run the synchronization at a more convenient time, using the Report Services Control Panel.

    c. Click **Finish** to close the configuration wizard.

       If the configuration was not successful, the configuration wizard provides some notes as to why the configuration failed. The notes may or may not include knowledge base articles that are available at the Delinea Technical Support web site.

Configuring a PostgreSQL Report Services Deployment

Follow these instructions if you're creating a new report services deployment using PostgreSQL or reconfiguring an existing PostgreSQL report services deployment.

To configure report services with a PostgreSQL database:

1. If you need to start the Delinea Report Services configuration wizard, go to the **Start** menu > **All Programs** > **Centrify Server Suite 2021.1** > **Report Services**, and choose **Configuration Wizard.**

   If you're continuing from the Delinea Management Services installer, the installer started the configuration wizard for you.
2. On the Welcome screen, click **Next** to continue.
3. If you have already set up report services, the Reconfiguring Report Services screen displays. Select **Reconfigure** and click **Next** to continue.
4. On the Database Type screen, select **PostgreSQL** and click **Next** to continue.
5. On the PostgreSQL screen, specify to create a new PostgreSQL installation or use an existing one.

   Because PostgreSQL doesn't have instances the way other databases do, Delinea recommends that you use an existing PostgreSQL database, if you already have one set up.

   For existing PostgreSQL installations, go to Step 8. Otherwise, for new installations, continue to Step 6.
6. To install a new PostgreSQL server, specify the PostgreSQL installer file location. You must specify a PostgreSQL installer version 11 or later. You can find the installer file in Common\PostgreSQL.

   Click **Next** to continue.
7. Specify the location of the PostgreSQL ODBC driver installer file. Delinea includes this file with the report services installer in Common\PostgreSQL.

   If you already have the official PostgreSQL ODBC drivers installed, this screen doesn't display.

   Click **Next** to continue.
8. Specify the PostgreSQL database settings:
   - **ODBC Driver**: For the PostgreSQL version that comes with report services, keep the default setting of PostgreSQL Unicode. This field can't be changed for new installations.
   - **Server**: If you're using an existing PostgreSQL server, enter the server name. For example, localhost or servername.acme.com.
   - **Port**: If you don't enter a port number, report services uses the default port 5432.
   - **Database**: This is the database name. The name can be up to 63 characters long, and the name cannot begin with an underscore (_) or dollar sign ($), and the instance name cannot contain any of the following special characters: a blank space, backslash (\), comma (,), colon (:), semi-colon (;), single quotation mark ('), ampersand (&), hyphen (-), number sign (#), or at sign (@).
   - **Database User**: This is your PostgreSQL administrator user. If you're using an existing PostgreSQL installation, the user must have the Create Database permission.
   - **Password**: This is the password for your PostgreSQL administrator user. If you're using an existing PostgreSQL installation, this is the password for the user with the Create Database permission.
   - **Confirm Password:** If you're creating a new installation, enter your password again to ensure the password is correct.

- **Additional Parameters**: Enter as needed. If you need to enter multiple characters, separate them with a colon (:).

  > The Configuration wizard verifies these settings after you've continued through all the configuration screens. Also, if you haven't installed the PostgreSQL ODBC driver, the Configuration wizard cannot verify these database settings.

9. If you selected domain-based reporting:
   a. In the Monitored Domain(s) screen, you can review and edit the list of domains that will be included for reporting. Add or remove domains as desired.

      For each domain, the configuration wizard lists the domain name and the domain controller name.

   b. Click **Next** to continue.
10. If you selected zone-based reporting and you use hierarchical zones:
    a. If you want data from all zones, select **Monitor all hierarchical zones from forest(s)**. You can add or edit forests by clicking **Edit** and then adding or removing forests.
    b. Or, if you want to report data from specific zones, select **Monitor only specific hierarchical zones**.
    c. Click **Edit**.

       The Specify Forest for zone selection dialog box opens.

    d. Enter the forest name where the desired zones are and click **OK**.

       The Edit Monitored Hierarchical Zones dialog box opens.

    e. Enter the hierarchical zones by name, or expand the list of zones to locate the desired zones manually.
    f. If desired, specify to select the parent or child zones automatically.
    g. Select the zone by putting a checkmark in the box next to the zone name.
    h. When you're done specifying which hierarchical zones to monitor, click **OK** to close the dialog box and return to the Configuration wizard.

       Each zone that you've selected is listed in the Hierarchical Zones screen.

    i. Click **Next** to continue.
11. If you selected zone-based reporting and you use classic zones:
    a. If you want data from all zones, select **Monitor all classic zones from forest(s)**. You can add or edit forests by clicking **Edit** and then adding or removing forests.
    b. Or, if you want to report data from specific zones, select **Monitor only specific classic zones**.
    c. Click **Edit**.

       The Specify Forest for zone selection dialog box opens.

    d. Enter the forest name where the desired zones are and click **OK**.

       The Edit Monitored Classic Zones dialog box opens.

e. Select the classic zones to include in your reports. Select the zone by putting a checkmark in the box next to the zone name.

   You can filter the list of zones by entering a portion of the name and clicking **Filter**.

f. When you're done specifying which classic zones to monitor, click **OK** to close the dialog box and return to the wizard. Click **Next** to continue.

12. For zone-based reporting, you can also specify which domain controller(s) that the report service connects to.

    If you don't specify which domain controller(s) to use, report services will use the default domain controller.

    a. Click **Add**.

       The Add Domain Controller dialog box opens.

    b. Enter the domain name and then select the domain controller from the list.

    c. Click **OK** to return to the Configuration wizard.

       The domain controllers that you selected are listed in the wizard screen.

    d. Click **Next** to continue.

13. In the Synchronization schedule screen, specify how often you want the reporting service to pull data from Active Directory.

    You can specify that the service synchronizes weekly, daily, every certain number of days, or every certain number of hours. The limit is 32,767 days or weeks.

    Click **Next** to continue.

14. Configure the user account that runs the service:

    a. In the Report Services options screen, specify the user account that will be used to run the service that synchronizes data from Active Directory and the reporting database.

       You can select a network service account, a managed service account, or another user account in Active Directory.

       You must specify a user account that has the required permissions. The configuration wizard verifies that the user has the correct level of access.

    b. Click **Next** to continue.

    c. The configuration wizard verifies that the specified user account has the required permission. An error displays if the permissions are inadequate.

    d. If the permission verification is successful, click **Close** to close the Verify permission window.

15. Review and complete the installation:

    a. In the Summary screen, review the installation details. If the installation settings are correct, click **Next** to continue.

       If you're installing a new database, it may take a few minutes.

    b. (Optional) In the completion screen, if the installation is successful, you can select the option to synchronize Active Directory data with the report database immediately. Depending on the Active Directory configuration

and domain size, this operation can take awhile to complete.

Or, alternatively, you can run the synchronization at a more convenient time, using the Report Services Control Panel.

c. Click **Finish** to close the configuration wizard.

If the configuration was not successful, the configuration wizard provides some notes as to why the configuration failed. The notes may or may not include knowledge base articles that are available at the Delinea Technical Support web site.

Delinea Report Services does not include a reporting solution for use with PostgreSQL.

Changing the Monitoring Mode for an Existing Report Services Deployment

You can easily switch from gathering report data based on domains or zones.

To change the monitoring mode for an existing report services deployment:

1. If you need to start the Delinea Report Services configuration wizard, go to the **Start** menu > **All Programs** > **Centrify Server Suite2021.1** > **Report Services**, and choose **Configuration Wizard.**

   If you're continuing from the Delinea Management Services installer, the installer started the configuration wizard for you.

2. On the Welcome screen, click **Next** to continue.
3. On the Reconfiguring Report Services screen, select **Switch the monitor mode** if you want to change whether report services uses domains or zones to synchronize Active Directory data. Click **Next** to continue.
4. On the Switch Monitor Mode screen, review the current and new mode settings. Click **Next** to continue.
   - To switch to domain-based reporting, go to Step 5.
   - To switch to zone-based reporting for hierarchical zones, go to Step 6.
   - To switch to zone-based reporting for classic zones, go to Step 7.
5. If you selected domain-based reporting:
   a. In the Monitored Domain(s) screen, you can review and edit the list of domains that will be included for reporting. Add or remove domains as desired.

      For each domain, the configuration wizard lists the domain name and the domain controller name.

   b. Click **Next** to continue.
6. If you selected zone-based reporting and you use hierarchical zones:
   a. If you want data from all zones, select **Monitor all hierarchical zones from forest(s)**. You can add or edit forests by clicking **Edit** and then adding or removing forests.
   b. Or, if you want to report data from specific zones, select **Monitor only specific hierarchical zones**.
   c. Click **Edit**.

      The Specify Forest for zone selection dialog box opens.

d. Enter the forest name where the desired zones are and click **OK**.

   The Edit Monitored Hierarchical Zones dialog box opens.

e. Enter the hierarchical zones by name, or expand the list of zones to locate the desired zones manually.

f. If desired, specify to select the parent or child zones automatically.

g. Select the zone by putting a checkmark in the box next to the zone name.

h. When you're done specifying which hierarchical zones to monitor, click **OK** to close the dialog box and return to the Configuration wizard.

   Each zone that you've selected is listed in the Hierarchical Zones screen.

i. Click **Next** to continue.

7. If you selected zone-based reporting and you use classic zones:

   a. If you want data from all zones, select **Monitor all classic zones from forest(s)**. You can add or edit forests by clicking **Edit** and then adding or removing forests.

   b. Or, if you want to report data from specific zones, select **Monitor only specific classic zones**.

   c. Click **Edit**.

      The Specify Forest for zone selection dialog box opens.

   d. Enter the forest name where the desired zones are and click **OK**.

      The Edit Monitored Classic Zones dialog box opens.

   e. Select the classic zones to include in your reports. Select the zone by putting a checkmark in the box next to the zone name.

      You can filter the list of zones by entering a portion of the name and clicking **Filter**.

   f. When you're done specifying which classic zones to monitor, click **OK** to close the dialog box and return to the wizard. Click **Next** to continue.

8. For zone-based reporting, you can also specify which domain controller(s) that the report service connects to.

   If you don't specify which domain controller(s) to use, report services will use the default domain controller.

   a. Click **Add**.

      The Add Domain Controller dialog box opens.

   b. Enter the domain name and then select the domain controller from the list.

   c. Click **OK** to return to the Configuration wizard.

      The domain controllers that you selected are listed in the wizard screen.

   d. Click **Next** to continue.

9. Configure the user account that runs the service:

   a. In the Report Services options screen, specify the user account that will be used to run the service that synchronizes data from Active Directory and the reporting database.

You can select a network service account, a managed service account, or another user account in Active Directory.

You must specify a user account that has the required permissions. The configuration wizard verifies that the user has the correct level of access.

b. Click **Next** to continue.

c. The configuration wizard verifies that the specified user account has the required permission. An error displays if the permissions are inadequate.

d. If the permission verification is successful, click **Close** to close the Verify permission window.

10. Review and complete the installation:

a. In the Summary screen, review the installation details. If the installation settings are correct, click **Next** to continue.

If you're installing a new database, it may take a few minutes.

b. (Optional) In the completion screen, if the installation is successful, you can select the option to synchronize Active Directory data with the report database immediately. Depending on the Active Directory configuration and domain size, this operation can take awhile to complete.

Or, alternatively, you can run the synchronization at a more convenient time, using the Report Services Control Panel.

c. Click **Finish** to close the configuration wizard.

If the configuration was not successful, the configuration wizard provides some notes as to why the configuration failed. The notes may or may not include knowledge base articles that are available at the Delinea Technical Support web site.

Installing and Configuring Report Services

This section includes the following topics:

- Before Installing - Prerequisites
- Installing Delinea Report Services
- Configuring Report Services and Deploying Your Reports
- Doing a Silent Install and Configuration
- Upgrading from a Prior Version
- Administering Delinea Report Services with the Report Control Panel
- Configuring SQL Server Reporting Services (SSRS)
- Re-deploying SQL Server Reports To SSRS

If you are deploying into a large Active Directory environment, be sure to also read Memory Recommendations and Requirements for large Active Directory environments.

Re-Deploying the SQL Server Reports to SSRS

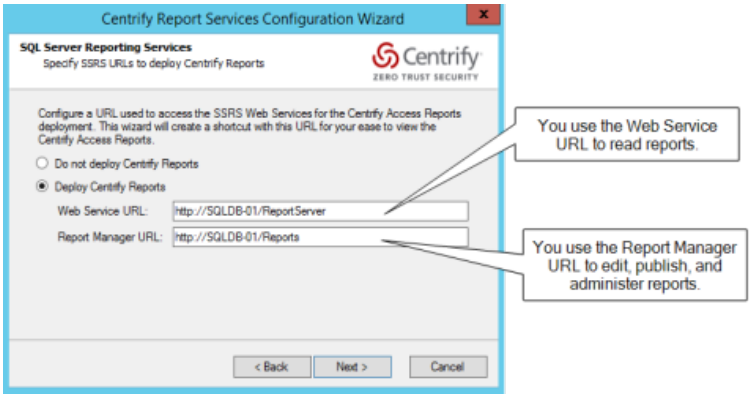
You can re-deploy your reports without needing to go through the entire Delinea Report Services configuration wizard. You can only re-deploy reports if you use SQL Server for your report database.

To configure Delinea report services using the configuration wizard:

1. If you need to start the Delinea Report Services configuration wizard, go to the **Start** menu > **All Programs** > **Centrify Server Suite 2021.1** > **Report Services**, and choose **Configuration Wizard.**

   If you're continuing from the Delinea Management Services installer, the installer started the configuration wizard for you.
2. On the Welcome screen, click **Next** to continue.
3. On the Reconfiguring Report Services screen, select **Deploy reports only** and click **Next** to continue.
4. Deploy the reports:
   a. In the SQL Server Reporting Services screen, specify whether to deploy the Server Suite reports (or not).

      If you plan to use a reporting solution other than Microsoft SQL Server Reporting Services, do not deploy the reports.



      This screen also lists the URLs for the Reporting Web Service and Report Manager. You'll use these URLs later to access to the reports.

      If you're using a production server of SQL Server and SSRS, you can configure them to use HTTPS. For details, see Microsoft SQL Server and SSRS documentation, such as https://msdn.microsoft.com/en-us/library/ms345223.aspx.

      The configuration wizard populates the report URLs automatically. If you had specified to use an existing SQL Server instance, the configuration wizard retrieves the existing web service URL and report manager URL for your SQL Server instance.

      For an existing SQL Server instance, you can open the Microsoft Reporting Services Configuration Manager to view the Web Service and Report Manager URLs.

   b. Click **Next** to continue.

      Review and complete the installation:

c. In the Summary screen, review the installation details. If the installation settings are correct, click **Next** to continue.

   If you're installing a new database, it may take a few minutes.

d. (Optional) In the completion screen, if the installation is successful, you can select the option to synchronize Active Directory data with the report database immediately. Depending on the Active Directory configuration and domain size, this operation can take awhile to complete.

   Or, alternatively, you can run the synchronization at a more convenient time, using the Report Services Control Panel.

e. Click **Finish** to close the configuration wizard.

   If the configuration was not successful, the configuration wizard provides some notes as to why the configuration failed. The notes may or may not include knowledge base articles that are available at the Delinea Technical Support web site.

Doing a Silent Install and Configuration

You can do what's called a silent install and configuration of Report Services, where you don't have to interact with a user interface and you plug in some configuration values ahead of time.

Doing a Silent Install of Report Services

Follow this procedure if you're installing Report Services components newly or upgrading to the latest version.

To silently install Report Services

1. Open a command window and run it as administrator.
2. Navigate to the Report Services folder in the installer package:

   Centrify-Server-Suite-**version**-mgmt-win64\DirectManage\Report Services

   where **version** refers to the Server Suite release version.
3. Run the following command to install the Report Services files:

   Centrify_RptServices-**version**-win64.msi /quiet

   where **version** refers to component version.

   The program installs the Report Services files into the default installation folder. You'll know that the install worked if you see newer files in that folder.

   You're now ready to configure Report Services. For new installations, see the next procedure. For upgrades, see Upgrading the reporting database silently.

Configuring a New Report Services Deployment Silently

There are a few main factors that drive which parameters to use in configuring Report Services silently (automatically without interaction):

- Are you creating a new database instance or publishing to an existing instance?
- Are you using PostreSQL or Microsoft SQL Server?

- Are you using Report Services in zone mode or domain mode?

When doing a silent configuration of report services, you create a file named config.json with the configuration parameters that you need for your deployment. For a list of the available parameters, see Report Services silent configuration parameters

Before you run the configuration program, be sure that you have the parameters set in the configuration file (config.json) and that you have the following ready to enter at the command line:

- ServiceAccount and ServiceAccountPassword
- PgSQLUser and PgSQLUserPassword (if using PostgreSQL)

The installer also supplies some sample configuration files (in the Report Services installation folder) that you can use as a guideline, depending on your deployment:

Database type	Domain mode	Zone mode
Microsoft SQL Server	config_sql_server_domain_mode_sample.json	config_sql_server_zone_mode_sample.json
PostgreSQL	config_postgresql_domain_mode_sample.json	config_postgresql_zone_mode_sample.json

To silently configure Report Services

1. Prepare the configuration file according to the settings you need.
2. Open a command line window as an administrator and run the report services configuration command according to the following usage:

```
Centrify.Report.Configuration.CLI.exe --ConfigFile "C:\\config.json" --ServiceAccount
"Local System" --ServiceAccountPassword --PgSQLUser --PgSQLUserPassword
```

Parameter	Description
`--ConfigFile`	The configuration json file, including the path. You can name this file as desired, as long as it's a .json file.
`--IsGroupManagedServiceAccount`	Use this option to specify that the service account is a group managed service account (gmsa).
`--ServiceAccount`	The service account to use to configure report services.
`--ServiceAccountPassword`	The service account password. If you're using a built-in account such as "Local System", you don't have to specify the password.
`--PgSQLUser`	If you use PostrgreSQL as your database, specify the PostreSQL user name
`--PgSQLUserPassword`	The PostgreSQL password

The command does the configuration. If there is an issue or error, the command displays a message in red text. When the configuration succeeds, there's a message in green text indicating that the configuration is done.

Report Services Silent Configuration Parameters

Use the following parameters in the Report Services configuration file (config.json). You don't need to use all of them; it depends on which kind of database you use and whether you're configuring Report Services in domain mode or zone mode. These parameters match what you would enter in the installer interface.

The installer also supplies some sample configuration files (in the Report Services installation folder) that you can use as a guideline, depending on your deployment:

Database type	Domain mode	Zone mode
Microsoft SQL Server	config_sql_server_domain_mode_sample.json	config_sql_server_zone_mode_sample.json
PostgreSQL	config_postgresql_domain_mode_sample.json	config_postgresql_zone_mode_sample.json

Parameter name	Parameter type	Description	Example
AdditionalParam	string	(PostgreSQL only) Use this parameter if you have any additional PostgreSQL parameters that you need to specify.	
DBInstallerPath	string	If you're creating a new database instance, this parameter specifies the location of the database installer file.	"DBInstallerPath": "D:\\Common\\SQLEXPR\\SQLEXPRADV_x64_ENU.exe"
DBInstallationPath	string	If you're creating a new database instance, this parameter specifies where to install the new database instance. For directories or path separators, use \\ instead of \.	"DBInstallationPath": "C:\\Program Files\\Microsoft SQL Server\\130"
DBName	string	If you're creating a new database instance, the name of the new database.	"DBName": "Report"
DomainControllers	dictionary	(Zone mode only) -- key = domain, value = domain controller	{"test.com": "dc.test.com"}

DomainMode		(Domain mode only) Use this parameter to specify domain mode. Inside of this parameter you specify the domains to synchronize to the reporting database.	"DomainMode": { "MonitoredDomains": { "test.com": "dc.test.com", "us.test.com": "dc.us.test.com" } }
ForestsForClassicZones	list of string values	(Zone mode only) The forest that contains the classic zones	
ForestsForHierarchicalZones	list of string values	(Zone mode only) The forest that contains the hierarchical zones	["companyA.com", "companyB.com"]
InstanceName	string	(SQL Server only) If you're creating a new database instance, the name of the new database instance. For directories or path separators, use \\ instead of \.	"InstanceName": "REPORTS"
IsDeployReport	true or false	(SQL Server only) Specifies whether or not to deploy reports.	"IsDeployReport": true
LogLevel	string	Specifies the amount of detail that the installer includes in the log file. The format of the parameter is as follows: `Log level (Off|Critical|Error|Warning|Information|Verbose|Trace)`	"LogLevel": "verbose"
MonitoredClassicZones (list)	list of string values	(Zone mode only) If you use classic zones, use this parameter to specify the list of zones to synchronize with report services.	["test.com/Program Data/Zones/ZoneC", "test.com/Program Data/Zones/ZoneD"]
MonitoredHierarchicalZones	list of string values	(Zone mode only) The list and location of hierarchical zones	["test.com/Program Data/Zones/hZoneA", "test.com/Program Data/Zones/hZoneB"]
NewDB	true or false	Specifies whether to create a new database instance or not	"NewDB": true
OdbcName	string	(PostgreSQL only) The name of the ODBC driver to use to connect with the PostgreSQL database.	"OdbcName": "PostgreSQL Unicode"
OdbcInstaller	string	(PostgreSQL only) The path and filename of the PostgreSQL installer file.	

Port	integer	(PostgreSQL only) The port for the PostgeSQL database. If you don't specify this parameter, the default port of 5432 is used.	"Port": "5432"
ReportManagerUrl	string	(SQL Server only) Specifies the report manager URL. You use this URL to edit, publish, and administer reports.	"ReportManagerUrl": "http://MYCOMPUTER/Reports_REPORTS"
ReportWebServiceUrl	string	(SQL Server only) Specifies the web service URL for deploying reports. You use the web service URL to read reports.	"ReportWebServiceUrl": "http://MYCOMPUTER/ReportServer_REPORTS"
ScheduleFrequency	integer	You use this parameter in conjunction with the ScheduleRule setting. With this parameter, you specify the number of hours, days, or weeks to configure how often the report synchronization will happen. For example, if you set ScheduleRule to weekly and you specify ScheduleFrequency to 1, the synchronization will happen every week. If you change the ScheduleFrequency to 3, the synchronization will happen every 3 weeks.	"ScheduleRule": "interval", "ScheduleFrequency": 2, The above example specifies that the report synchronization will happen every 2 hours.

string	You use this parameter in conjunction with the ScheduleFrequency setting. With this parameter, you specify what sets of time to count when scheduling the frequency of report services synchronization. The options that you can specify are "daily", "interval", or "weekly". Interval specifies an hourly interval.	"ScheduleRule": "weekly", "ScheduleFrequency": 2, The above example specifies that the report synchronization will happen every 2 weeks.	
ScheduleStartTime (string)	string	Specifies the time of day to start the report services synchronization, in the 24 hour format of hh:mm:ss.	"ScheduleStartTime": "14:00:00",
ScheduleWeekDays (list)	list of string values	Specifies on which days of the week the report services synchronization will happen. You can specify "all" for a daily synchronization or "none" to just do it manually as needed. Otherwise, you can specify one or more of the following for days of the week: "mon", "tue", "wed", "thu", "fri", "sat", "sun"	"ScheduleWeekDays": ["mon", "wed", "fri"]

Server	string	(PostgreSQL only) The name of the PostgreSQL server.	"Server":"localhost"
SqlCmdTimeout	int	SqlCommand timeout (second)	"SqlCmdTimeout": 3300
ZoneMode		(Zone mode only) Use this parameter to specify zone mode. Inside of this parameter you specify the MonitoredClassicZones and the MonitoredHierarchicalZones parameters and their respective settings.	ZoneMode": { "MonitoredClassicZones": [], "MonitoredHierarchicalZones": ["test.com/Program Data/Zones/hZoneA"], "ForestsForClassicZones": ["test.com"], "ForestsForHierarchicalZones": [], "DomainControllers": { "test.com": "dc.test.com", "us.test.com": "dc.us.test.com" } }

Upgrading from a Prior Version

You can install or upgrade the report services components using the Delinea Management Services installer and then use either the Report Services Configuration wizard or the Database Upgrade and Deployment wizard to get your database and reports set up. This table highlights which tools you can use, depending on whether you have a previous version of report services installed or not.

Do you have a previous version of report services installed?	Run the Server Suite installer to do this	Then do this to get your database and reports set up
No	Install the report services components	Run the Configuration wizard to configure report services and deploy reports. For details, see Configuring Report Services and Deploying your Reports
Yes	Upgrade your report services components.	Run the Database Upgrade and Deployment wizard to upgrade your report database and deploy reports. For details, see Upgrading your report services database.

If you're upgrading from a version of Server Suite prior to 2016 or you don't currently have report services installed, you'll need to specifically indicate during the installation when you want to install the report services components - they aren't installed by default during an upgrade.

The Access Manager reports are still available, wherever you've installed Access Manager. Report services are in addition to the standard Access Manager reports.

Upgrading Your Report Services Database

If you're upgrading from a previous release of report services, you need to make sure that your report database is up to date. You'll also need to deploy your reports again so that they are based on the updated database.

The following SQL Server permissions are required in order to upgrade the report database with the Upgrade and Deployment wizard:

- Execute stored procedure permission on report database
- Create schema permission on report database
- Create table permission on report database
- Create view permission on report database
- Create stored procedure permission on report database
- Create type permission on report database
- Alter any schema permission on report database
- Insert, Delete, Update, Select and Execute permissions on the schema "Dbo", "RawData", "ReportData", "ReportView" and "ConfigData" on report database

In order to deploy reports, you must have the Microsoft SQL Server Reporting Services role of Content Manager. For details for how to grant SSRS roles, see Granting access in SSRS to reports.

To upgrade your report database:

1. From the Start menu, locate and run the **Delinea Report Services Upgrade and Deployment wizard**.
2. In the initial screen, click **Next** to continue.
3. The wizard upgrades the database automatically.

   The database upgrade changes are saved to the database after you exit the wizard later.
4. If you have deployed reports before, configure where to back up the existing reports and where the new reports will be deployed.

   If you haven't deployed reports before, you're prompted to specify where to deploy reports.

   If desired, you can select the option to not backup nor deploy reports.

   Click **Next** to continue.
5. In the Summary screen, review the settings and if they're correct, click **Next** to continue.

   The wizard upgrades your report database.
6. In the completion screen, click **Finish** to exit the wizard.

   (If the upgrade failed for any reason, the Summary screen displays some details about why the upgrade failed.)

   Your report database is updated and your reports are deployed, if you specified the option to do so.

> After upgrade, you should perform a full synchronization before an incremental update is allowed. (Ref: CS-40029a)

Upgrading from Versions Before 2016

As of Server Suite 2016 the report services feature provides reports. If you're upgrading from a version prior to release 2016 and you're accustomed to the Access Manager reports, this section covers the differences between the reports.

If you want to know which Delinea report services reports correspond to the Access Manager reports, below is a list. The reports are listed according to the Access Manager report so that you can easily determine which new report you want to use instead.

Classic Zone Access Manager Reports

These Classic Zone reports correspond to the report services reports as follows:

Access Manager report name	Includes this information by default	Delinea report services report name
Classic Zone - Authorization Report for Computers	Lists each computer in the zone and indicates which users are allowed to access each computer.	Authorization Report
Classic Zone - Authorization Report for Users	Lists each user account in the zone and indicates which computers each user can access.	
Classic Zone - User Privileged Command Rights Grouped by Zone	Lists the privileged commands that each user has permission to run and the scope to which the user's rights apply.	Classic Zone - User Privileged Command Rights Report
Classic Zone - User Role Assignments Grouped by Zone	Lists the role assignments for each user in each zone.	Classic Zone - User Role Assignment Report
Classic Zone - Users Report	Lists information from the UNIX profile for each user in each classic zone.	
Classic Zone - Zone Role Privileges	Lists the roles that are defined for each classic zone and the rights granted by each of these roles.	Zone Role Privileges Report

Hierarchical Zone Access Manager Reports

These Hierarchical Zone reports correspond to the report services reports as follows:

Access Manager report name	Includes this information by default	Delinea report services report name
Hierarchical Zone - Computer Effective Audit Level	Lists the audit level in effect for computers in each zone.	Hierarchical Zone - Effective Audit Level

Hierarchical Zone - Computer Effective Rights	Lists the privileges granted on each computer.	Hierarchical Zone - Effective Rights Report
Hierarchical Zone - UNIX User Effective Rights	Lists the effective rights for each UNIX user on each computer. The report shows the name of the right, it's type, and where it is defined.	
Hierarchical Zone - Windows User Effective Rights	Lists the effective rights for each Windows user on each computer. The report shows the name of the right, it's type, and where it is defined.	
Hierarchical Zone - Computer Effective Roles	Lists the roles assigned on each computer.	Hierarchical Zone - Effective Role Report
Hierarchical Zone - Computer Role Assignments	Lists the computer roles that are defined for each zone. The report includes the users and groups and their associated roles.	Hierarchical Zone - Computer Role Assignments Report
Hierarchical Zone - Computer Role Membership	Lists the computer roles that are defined for each computer and the zone to which they belong.	Hierarchical Zone - Computer role Membership Report
Hierarchical Zone - Computer Role Membership Grouped by Zone	Lists the computer roles that are defined for each computer grouped by the zone to which they belong.	

All Zone Access Manager Reports

These reports correspond to report services reports as follows:

Access Manager report name	Includes this information by default	Delinea report services report name
Computer Summary Report	Lists computer account information for each computer in each zone.	Computers Summary Report
Computers Report	Lists computer account information for each computer in each zone.	
Groups Report	Lists group information for each group in each zone.	Groups Report

Stale Computers Report	Lists the stale computers.	Stale Computers Report
User Accounts Report	Lists account details for the users that have UNIX profiles in each zone. The report includes the Active Directory display name, the Active Directory login name, the Active Directory domain for the account, and details about the account status, such as whether the account is configured to expire, locked out, or disabled and the date and time of the account's last login.	User Accounts Report
Zones Report	Lists the zone properties for each zone. The report includes the zone name, list of available shells, the default shell, the default home directory path, the default primary group, the next available UID, reserved UIDs, the next available GID, and reserved GIDs.	Zones Report

Reports that are New to Access Manager Report Users

In addition to converting the content of the Access Manager reports into the report services reports, there are also the following new reports:

- Hierarchical Zone - Computer Role Effective Assignments Report (one for UNIX, one for Windows)
- Hierarchical Zone - Zone Effective Assignments Report (one for UNIX, one for Windows)
- Attestation reports for SOX and PCI compliance

Upgrading the Reporting Database Silently

If desired, you can upgrade your report services database without any user interaction, after you install the latest version of the Report Services components. You supply any of the parameters in the table below when you run the command line program. These parameters match the settings in the Upgrade and Deployment wizard.

Parameter name	Parameter type	Description	Example
ReDeployReport	switch	Specifies whether or not to redeploy reports after you upgrade the database. If you include this parameter, the service will redeploy reports. If you don't include this parameter, the service doesn't redeploy reports.	`--ReDeployReport`

ReportBackupFolder	string	Specifies the path and folder location to backup existing reports before upgrading. This option only applies if you specify ReDeployReport to yes. If you don't specify a value for this property, the service uses the default value of "Backup reports".	
WebServiceURL	string	Specifies the web service URL for deploying reports. You use the web service URL to read reports. If you don't specify this value, the service uses the current setting.	"ReportWebServiceUrl": "http://server1/ReportServer_REPORTS"
ReportManagerURL	string	Specifies the report manager URL. You use this URL to edit, publish, and administer reports. If you don't specify this value, the service uses the current setting.	"ReportManagerUrl": "http://server1/Reports_REPORTS"

To silently upgrade Report Services:

1. Install the latest version of the Report Services components. For details, see Silently installing Report Services.
2. At the command line (be sure to run as administrator), run the following command with the desired upgrade parameters, as listed in the table above. None of the parameters are mandatory.

   ```
   Centrify.Report.Upgrade.Cli.exe --ReDeployReport --ReportBackupFolder "previous-reports"
   ```

   The upgrade program lists out each upgrade task that it performs as it progresses. When the program finishes, there's a message that says the upgrade is finished.

Building Custom Reports

You can build your own reports with data from the Delinea report services database by using your own reporting tool or Microsoft SQL Server Reporting Services.

Requirements and Recommendations

In order to build your own reports or customize existing reports, you also need to have the SSRS Report Builder installed where you have SSRS installed.

Known Limitations and Recommendations

- Use the same domain where Microsoft SSRS is installed. If you try to use SSRS in a domain that is different from the domain where SSRS is installed, you may have some difficulty accessing reports. For example, if your computer runs in the acme.com domain and you have SSRS installed in a test domain of wiley.coyote.com, you may run into issues accessing the reports.
- If you're accessing SSRS from a different domain, make sure that you enter your credentials and save them.
- When you log in to SSRS, make sure that the user you're logging in as has at least the system user role, and at least read access to the folder (according to the folder settings in SSRS).

An Overview of Report Building Tasks

Microsoft documentation contains specific instructions for how to create custom reports using SSRS Report Builder. Included here is the overall process; please consult Microsoft SSRS Report Builder documentation for details.

For example, here's a link to Microsoft information on using SQL Server Reporting Services 2012: https://technet.microsoft.com/en-us/library/hh338693.aspx.

An overview of how to build custom reports using SSRS and Delinea report services data:

1. Open Internet Explorer to the deployed reports URL.
   - Make sure that you have the correct access permissions in SSRS for building reports. For details, see Granting Access in SSRS to Reports.
   - It's recommended that you log in to the deployed reports URL as a user with Report Building permissions, but not database administrator permissions. If you log in as a user with access to all tables in the reporting database, you may see tables that you cannot use in custom reports. Delinea exposes the views for you to use in your custom reports.
2. Open Microsoft SQL Server Report Builder, and create the dataset that connects you to the reporting data source.

   (The dataset is the set of data retrieved from the database, and the data source is the connection information for the database.)
3. Create a new report that's based on the data set that you just created.
4. Design a query using the provided views.
5. Run the report to make sure that you get data in the report.
6. Edit the report as desired.
7. Save the report.

   Microsoft SSRS saves the report as a .RDL file.
8. Publish the report by publishing the RDL file.

Migrating Custom Reports from SQL Server Express

If you create custom reports using the included version of SQL Server 2008 R2 Express edition, you can migrate those custom reports over to a production SQL Server. You'll need to download each custom report and then re-upload them into the production system.

To download your custom reports from SQL Server Express:

1. Create a temporary folder on your local computer.

   You'll use this folder to store your downloaded custom reports temporarily.
2. Open Delinea Report Services in Internet Explorer.
3. Navigate to the Custom Reports folder.
4. Select a report and select **Download** from the report's action menu.
5. Save the downloaded report in the temporary folder that you already created.

   Repeat this process for each report.
6. Close Internet Explorer.

To upload your custom reports to your production instance of SQL Server:

1. Run the Delinea Report Services Configuration wizard.
2. In the configuration wizard, choose the production SQL Server instance where you want to deploy the reports, then close the wizard.
3. Open Delinea Report Services in Internet Explorer.
4. Navigate to the Custom Reports folder.
5. For each report:
   a. Click **Upload File** and select the custom report that you downloaded from your other instance.
   b. After the report is uploaded, select the report and click **Manage**.
   c. Click the **Data Sources** tab.
   d. Select **A shared data source** and click **Browse**.
   e. In the folder listing, expand the **Centrify Report Services** folder.
   f. Select **ReportDataSource** and click **OK**.
   g. In the Data Sources page, click **Apply**.

You can now open the custom report successfully using data in your production SQL Server instance.

Viewing Default Reports

This section covers how to open a report, and provides some basic information on each of the default reports.

Opening a Report

You open a report by going to the report folder URL in Internet Explorer. Click a report to open it.

In general, you and your users access the reports from a URL. The URL has a format like this:

"http://hostname/Reports_reportDBname"

Filtering Report Data by Zone

When you view a report, you can filter the report data by zone. In the zone drop-down filter, report services lists each zone by its full zone hierarchy, so that you can choose based on parent or child zones. For example, if you have a child zone named California as part of a parent zone West which is part of the parent zone United States, the zone appears in the list as "United States/West/California.

Zones are listed in the zone drop-down filter in alphabetical order, and the first zone in the list is the default zone. When you first open a report, report services initially generates the report data based on the default zone.

Default Access Manager Reports

Report Services Reports: Not Specific to Classic or Hierarchical Zones

Report Name	Report description	Filter the results with these fields
Authorization report	This report lists each computer or user account, and which users are allowed to access each computer.	Access Level Computer domain Computer Name User domain User name User Type Zone Zone domain
Computers Summary report	Lists computer account information for each computer in each zone.	Computer domain Computer name Platform Zone Zone domain Zone type
Delegation report	Lists which users, groups, computers, group managed service accounts (gMSA), managed service accounts (MSA), and which well-known SIDs have which delegation tasks.	Delegation Task Target Target Domain Target Name Trustee Trustee Domain Trustee Type Zone
Effective delegation report	Lists which Active Directory users, Active Directory groups, group managed service accounts (gMSA), and managed service accounts (MSA) have which delegation tasks.	Active Directory User Domain Active Directory User Name Delegation Task Target Target Domain Target Name Zone

Groups report	Lists group information for each group in each zone, including the Active Directory group name, the UNIX group name, the UNIX group identifier (GID), and whether the group is an orphan. If the group is for local users, the local group status indicates whether the group is enabled or disabled for local access.	Active Directory Group name Active Directory Group domain Group Type Is Orphan Local Group Status UNIX Group Name Zone Zone Domain Zone Type
Stale Computers report	Lists the stale computers. Stale computers are those where the password hasn't changed for 90 or more days.	Computer Domain Computer Name Zone Zone domain
User Accounts Report	Lists account details for Active Directory users who are related to each zone. The report includes the Active Directory display name, the Active Directory login name, the Active Directory domain for the account, and details about the account status, such as whether the account is configured to expire, locked out, or disabled and the date and time of the account's last login.	Active Directory user name Domain Enabled
Users Report	Lists user information for each user in each zone. If the user is a local user, the local user status indicates whether the user is enabled or disabled for local access.	Active Directory user Active Directory user domain UNIX name Enabled Is Orphan Local User Status User Type Zone Zone domain Zone type
Zone Role Privileges Report	Lists the roles that are defined for each hierarchical zone and the rights granted by each of these roles.	Right name Right type Role name Zone Zone domain Zone type
Zones Report	Lists the administrative tasks and properties for each zone and the users or groups have been delegated to perform each task. This report indicates which users or groups have permission to perform specific tasks, such as add groups, join computers to a zone, or change zone properties.	Zone Zone domain

Delinea Report Services Reports: Classic Zone Reports

New default report	New report description	Filter the results with these fields

Classic Zone - User Privileged Command Rights Report	Lists the privileged commands that each user has permission to run and the scope to which the user's rights apply.	Classic zone Privileged command name User name Zone domain
Classic Zone - User Role Assignment Report	Lists information from the UNIX profile for each user in each classic zone. Lists the role assignments for each user in each zone. The report includes the domain name, user profile name, the list of roles the user is assigned to in each zone, and the scope to which the user's role assignment applies.	Classic zone Role User domain User name Zone domain

Delinea Report Services Reports: Hierarchical Zone Reports

New default report	New report description	Filter the results with these fields
Hierarchical zone - Computer Role Assignments Report	Lists the computer roles that are defined for each zone. The report includes the users and groups and their associated roles.	Role name Computer Role name Zone Zone domain
Hierarchical zone - Computer Role Effective Assignments Report	Lists the roles assigned on each computer. There are separate reports for UNIX and Windows computers.	Computer role Right Right type Role User Domain User Name Zone Zone Domain
Hierarchical Zone - Computer Role Membership Report	Lists the computer roles that are defined for each computer and the zone to which they belong.	Computer Domain Computer Name Computer Role in Zone Computer Role Name Join To Zone Domain
Hierarchical Zone - Effective Audit Level Report	Lists the audit level in effect for computers in each zone.	computer domain computer name User domain user name zone zone domain
Hierarchical Zone - Effective Rights Report	Lists the privileges granted on each computer and the effective rights for each Windows and UNIX user on each computer.	computer domain computer name Right Right type Role User domain user name zone zone domain

Hierarchical Zone - Effective Role Report	Lists the role assignment on each computer in the zone.	computer domain computer name Role User domain user name zone zone domain
Hierarchical Zone - Users Report	Lists the users and the computers to which they have access in the zone. If the user is a local user, the local user status indicates whether the user is enabled or disabled for local access.	Active Directory user Active Directory user domain Computer Computer domain Is orphan Is secondary Local User Status UNIX name User type Zone Zone domain
Hierarchical Zone - Zone Effective Assignments Report	Lists the roles that are defined for each hierarchical zone and the rights granted by each of these roles, including where each right is defined. There are separate reports for UNIX and Windows users.	Right Right type Role User domain user name zone zone domain

Default SOX Attestation Reports

To help your department comply with Sarbanes-Oxley audit requirements, Delinea provides some default SOX reports. These reports show you who has access to computers, what roles and rights users have, and similar data that's needed to show SOX compliance.

SOX reports provide the following kinds of information:

- **Computers**: Who has access to these computers, what are the roles, rights, and groups that they belong to
- **Groups**: Which users are in which groups, what are the roles, rights, and what computers can these users access
- **Users**: What their role assignments are, what rights the users have, which groups they belong to, and which computers they have access to
- **Roles**: Which computers the rules have access to, what rights are assigned to the group, and which groups are assigned to which roles

You can find the SOX reports in SSRS by going to the Centrify Report Services > Attestation > SOX reports folder.

> In larger environments, you can save processing time when running an attestation report (PCI or SOX report) by choosing to exclude the chart from the report. When you open the report, select **True** for the **Exclude chart for faster report generation** option.

For a description of how report services calculates the data for the charts in the SOX reports, see How objects are counted for the PCI and SOX report charts.

Here is a list of the SOX reports, along with a brief description and how you can filter the results.

Report name	Report description	Filter the results with these fields
SOX - Login Report - By Computer	For each computer, this report displays the users who can log in. For each user who can log in, the report shows the role, assignment location, and assignee.	Computer Computer group Computer role Zone Zone Domain Zone Type
SOX - Login Report - By Group	For each Active Directory group, this report lists the computers and role assignment information.	Active Directory group Zone Zone Domain Zone Type
SOX - Login Report - By Role	For each role, this report lists the computers assigned to that role.	Role Zone Zone Domain Zone Type
SOX - Login Report - By User	For each user, this report lists the computers that the user can access as well as the role assignment information.	User Zone Zone Domain Zone Type
SOX - Login Summary Report	This report provides a summary of who can log in to which computer.	Computer Computer group Computer role Local User Status User User group User type Zone domain Zone type Zone
SOX - Rights Report - By Computer	For each computer, this report lists the users who have which login and other privileges and what the role assignments are.	Computer Computer Group Computer role Right type Zone Zone Domain Zone Type
SOX - Rights Report - By Group	For each Active Directory group, this report lists the computers have which login and other privileges and what the role assignments are.	Active Directory group Right type Zone Zone Domain Zone Type
SOX - Rights Report - By Role	For each role, this report lists the computer and rights available on that computer.	Role Zone Zone Domain Zone Type
SOX - Rights Report - By User	For each user, this report lists the Active Directory group, computers, and role assignment.	Right type User Zone Zone Domain Zone Type

SOX - Rights Summary Report	This report provides a summary of which rights are granted to which users on which computers.	Computer Computer group Computer role Local User Status Right type User group User User type Zone Zone Domain Zone type

When you view the collection of reports in Internet Explorer, you may also see some sub-reports listed. These are not actual reports but views that support the actual reports; due to a limitation with Microsoft SSRS, these sub-reports may display even though they're not meant to be used. Please do not click any reports that have names that begin with SubReport.

In these reports, Computer Role and Computer Group filters return records assigned to those roles or groups but not where the role assignment is defined. For example, if you filter records for Zone1_CompRoleA, the report lists all computers that are in the computer role named Zone1_CompRoleA.

The charts in the PCI & SOX reports do not consider role assignments that are granted to "All Active Directory Users," and the reports only consider role assignments that are granted to specific users and groups when counting computer access and privileges. On the other hand, the detailed report shows all the login and privilege information from all role assignments (including those that are granted to "All Active Directory Users").

Default PCI Attestation Reports

To help your department comply with PCI audit requirements, Delinea provides some default PCI attestation reports. These reports show you who has access to computers, what roles and rights users have, and similar data that's needed to show PCI compliance.

PCI reports provide the following kinds of information:

- Computers: Which users have access to these computers, what are their roles and rights
- Groups: Which users are in which groups, what are their roles and rights, and which computers do they have access to
- Users: What role is the user assigned to, what rights does the user have, and which computers does the user have access to
- Roles: What computers do these roles have access to and what rights do they have

You can find the PCI reports in SSRS by going to the Centrify Report Services > Attestation > PCI reports folder.

In larger environments, you can save processing time when running an attestation report (PCI or SOX report) by choosing to exclude the chart from the report. When you open the report, select **True** for the **Exclude chart for faster report generation** option.

For a description of how report services calculates the data for the charts in the PCI reports, see How objects are counted for the PCI and SOX report charts.

Here is a list of the PCI reports, along with a brief description and how you can filter the results.

Report name	Report description	Filter the results with these fields
PCI - Login Report - By Computer	For each computer, this report displays the users who can log in. For each user who can log in, the report shows the role, assignment location, and assignee.	Computer Computer group Computer role Zone Zone Domain Zone Type
PCI - Login Report - By Group	For each Active Directory group, this report lists the computers and role assignment information.	Active Directory group Zone Zone Domain Zone Type
PCI - Login Report - By Role	For each role, this report lists the computers assigned to that role.	Role Zone Zone Domain Zone Type
PCI - Login Report - By User	For each user, this report lists the computers that the user can access as well as the role assignment information.	User Zone Zone Domain Zone Type
PCI - Login Summary Report	This report provides a summary of who can log in to which computer.	Computer Computer group Computer role Local User Status User User group User type Zone domain Zone type Zone
PCI- Rights Report - By Computer	For each computer, this report lists the users who have which login and other privileges and what the role assignments are.	Computer Computer Group Computer role Right type Zone Zone Domain Zone Type
PCI- Rights Report - By Group	For each Active Directory group, this report lists the computers have which login and other privileges and what the role assignments are.	Active Directory group Right type Zone Zone Domain Zone Type
PCI- Rights Report - By Role	For each role, this report lists the computer and rights available on that computer.	Role Zone Zone Domain Zone Type
PCI- Rights Report - By User	For each user, this report lists the Active Directory group, computers, and role assignment.	Right type User Zone Zone Domain Zone Type
PCI - Rights Summary Report	This report provides a summary of which rights are granted to which users on which computers.	Computer Computer group Computer role Local User Status Right type User group User User type Zone Zone Domain Zone type

When you view the collection of reports in Internet Explorer, you may also see some sub-reports listed. These are not actual reports but views that support the actual reports; due to a limitation with Microsoft SSRS, these sub-reports may display even though they're not meant to be used. Please do not click any reports that have names that begin with SubReport.

In these reports, Computer Role and Computer Group filters return records assigned to those roles or groups but not where the role assignment is defined. For example, if you filter records for Zone1_CompRoleA, the report lists all computers that are in the computer role named Zone1_CompRoleA.

The charts in the PCI & SOX reports do not consider role assignments that are granted to "All Active Directory Users," and the reports only consider role assignments that are granted to specific users and groups when counting computer access and privileges. On the other hand, the detailed report shows all the login and privilege information from all role assignments (including those that are granted to "All Active Directory Users").

How Objects are Counted for the PCI and SOX Report Charts

This section describes how objects are counted for the charts that you see in the PCI & SOX reports.

Login Report Charts

In login reports, we count how many computers each user can log in to, how many users can log in to each computer, and how many roles are granted with login rights.

In hierarchical zones, a role is considered to be granted with a login right if one or more of the following rights are granted to the role:

- Console login is allowed
- Remote login is allowed
- Password login and non-password login are allowed
- Non password login is allowed

In classic zones, a role is considered to be granted with a login right if at least one PAM right is granted to the role.

In the graphs that report the number of users who can log in to a computer, or the number of computers that a user is logged in to; the graphs only consider effective users. An effective user is one who has a complete user profile in a classic zone. In hierarchical zones, an effective user must also have been granted the login right through any role that is assigned to users/groups. Note that a "login right" obtained from a role that is assigned to "All AD users" is not considered in the graphs.

A local user is counted as an effective user in hierarchical zones if the user is granted the "User is visible" right from any effective role assignment.

Login Report – By Computer charts

Computers with Most Access chart

This chart ranks the computers by the number of effective users and shows the top 10 computers.

User Roles Count for Computers with Most Access chart

This chart ranks the computers by the number of roles that assign login rights to users or groups on the computer.

Users with Most Access chart

This chart ranks the users by the number of computers that each one can log in to, and shows the top 10 users.

Login Report – By Group charts

Roles with Most Access chart (by Group)

This chart ranks all the roles that are assigned to any group by the number of computers that the role grants login access to (regardless of how many groups are assigned to each role), and shows the top 10 roles.

Groups with Most Members chart

This chart shows the top 10 groups that have most members, including those from nested groups.

Login Report – By Role charts

Roles with Most Access chart (by Role)

This chart ranks all the roles that are assigned by the number of computers that the role grants login access to, and shows the top 10 roles.

Roles with Most Users chart

This chart ranks the number of users for which each role is effective (regardless of the role assignment scope), and shows the top 10 roles.

Roles with Most Rights chart

This chart ranks the assigned roles (regardless of the role assignment scope) with login rights by the number of granted privilege access rights.

Login Report – By User charts

Users with Most Access On Computers chart

This chart ranks the users by the number of computers that each one can log into, and shows the top 10 users.

Login Roles Count for Users with Most Access On Computers chart

This chart ranks the users by the number of effective roles that grant login access to any computer, and shows the top 10 users.

Login Summary Report charts

Computers With Most Access chart

This chart ranks the computers by the number of effective users and shows the top 10 computers. Both Active Directory and local effective users are considered.

Users With Most Access chart

This chart ranks all effective users by the number of computers that each user can log into, and shows the top 10 users.

Rights Report Charts

In each rights report, the privileged access right enables the user to create additional working environments or to run specified applications with different privileges. The following five privileged access rights are included in rights reports.

- Network Access right
- Desktop right
- Application right
- Commands
- Use restricted environment

Each privileged access right is counted in the reports only when the role with one of these rights is assigned to users and/or groups. However, the privileged right granted using ‘All AD user’ is not counted.

Rights Report – By Computer Charts

Computers with Most Privileged Access chart

This chart ranks the computer by the number of distinct privileged access rights that are effective on each computer, and shows the top 10 computers. A privileged access right is counted as one regardless of the number of users or roles that is granted or assigned the right in the computer.

Computer Roles with Most Privileged Access Chart

This chart ranks all the computer roles by the number of distinct privileged access rights assigned to each computer role, and shows the top 10 computer roles.

Privileged Access with Most Computers Chart

This chart ranks all privileged access rights by the number of computers that each right is effective on, and shows the top 10 rights.

Rights Report – By Group Charts

Groups with Most Privileged Access Chart

This chart ranks the group by the number of distinct privilege access rights granted to each group, and shows the top 10 groups. The privilege access rights are evaluated based on all roles that are assigned to groups, regardless of the scope of the assignments.

Rights Report – By Role Charts

Computer Roles with Most Privileged Access Chart

This chart ranks all the computer roles by the number of distinct privileged access rights assigned to each computer role, and shows the top 10 computer roles.

User Roles with Most Privileged Access Chart

This chart ranks the assigned roles (regardless of the role assignment scope) with login rights by the number of granted privileged access rights.

Rights Report – By User Charts

Users with Most Privileged Access Chart

This chart ranks all users by the number of distinct privileged access rights granted (regardless of the number of computers) and shows the top 10 users.

Computer Role Count for Users with Most Privileged Access Chart

This chart ranks all users by the number of distinct privilege access rights granted. For the top 10 users, it shows the number of computer roles where the user is assigned to any role in that computer role.

Rights Summary Report Charts

Computers with Most Privileged Access Chart

This chart ranks the computer by the number of distinct privileged access rights that are effective on each computer, and shows the top 10 computers. A privileged access right is counted as one regardless of the number of users or roles that is granted or assigned the right in the computer.

Users with Most Privileged Access Chart

This chart ranks all effective users by the number of distinct privileged access rights granted (regardless of the number of computers) and shows the top 10 users.

Most Dominant Privileges on Computers chart

This chart ranks all privileged access rights by the number of computers that each right is effective on and shows the top 10 rights. The number of users where the right is effective in each computer is not considered in the ranking.

Configuring Report Services for Large Active Directory Environments

Configuration issues can significantly affect the performance of synchronizing Active Directory information and report queries and generation. This section describes additional considerations for deploying Delinea Report Services successfully in a large Active Directory environment.

Memory Recommendations and Requirements for Large Active Directory Environments

Domain Controller Memory

Symptoms

The domain controller runs slower or stops responding.

You can use the Performance monitor tool to evaluate if the system is operating within adequate capacity thresholds.

For details, see: http://social.technet.microsoft.com/wiki/contents/articles/14355.capacity-planning-for-active-directory-domain-services.aspx#Monitoring_For_Compliance_With_Capacity_Planning_Goals

Resolution

Ensure the system has a sufficient amount of RAM. The minimum amount of RAM should be the sum of:

- Active Directory database size (such as the size of the C:\Windows\NTDS\ folder)
- Total SYSVOL size (such as the size of the C:\Windows\SYSVOL folder)
- Operating system recommended amount of RAM
- Vendor recommendations for the agents (antivirus, monitoring, backup, and so on)
- Additional amount of RAM to accommodate growth over the lifetime of the server.

For details, see: http://social.technet.microsoft.com/wiki/contents/articles/14355.capacity-planning-for-active-directory-domain-services.aspx

Windows Memory Requirements

Here are the memory requirements for different versions of Windows:

Windows version	Minimum memory required
Windows 2008, 2008 R2	512 MB minimum 2 GB or more is recommended
Windows 2012, 2012 R2	512 MB minimum
Windows 7, 8, 8.1, 10	2 GB minimum for 64-bit systems

References

http://windows.microsoft.com/en-us/windows7/products/system-requirements

http://windows.microsoft.com/en-US/windows-8/system-requirements

http://www.microsoft.com/en-us/windows/windows-10-specifications

https://technet.microsoft.com/en-us/windowsserver/bb414778.aspx

https://technet.microsoft.com/en-us/library/dn303418.aspx

Sql Server Memory

Symptoms

- Delinea Report Services fails to rebuild or refresh a snapshot because of insufficient system memory or an out of memory error.
- You cannot open reports in SSRS because of insufficient system memory or an out of memory error.

Resolution

Ensure that your SQL Server deployment has sufficient memory. Different versions of SQL Server have different memory requirements. For details, please see:

https://msdn.microsoft.com/en-us/library/ms143506.aspx

In addition to Microsoft's recommended memory requirement for SQL Server, an additional amount of memory is required for SQL Server in order to rebuild/refresh snapshot data and render the report successfully.

For more information, see Configuration Recommendations for Large Active Directory Environments.

Configuration Recommendations for Large Active Directory Environments

The major factor of evaluating the configuration requirements for SQL Server is the total number of effective users who can access the computers that are joined to zone in the Active Directory environment. You can estimate the total number of effective users by multiplying the number of computers joined to the zone by the average number of users who can access the computer.

Below lists the recommended configurations for SQL Server for some sample Active Directory environments.

Active Directory environment Sample #1:

Number of computers joined to a zone	1000
Average number of users who can access the computer	500
Total number of effective users	500 * 1000= 500,000
90% of user profiles and role assignments are explicitly defined at the zone level	

Active Directory environment Sample #1 configuration recommendations :

SQL Server edition	SQL Server Express Edition with Advanced Services
SQL Server memory	8 GB
SQL Server disk space	30 GB

Active Directory environment Sample #2:

Number of computers joined to a zone	5,000
Average number of users who can access the computer	3,000
Total number of effective users	3,000 * 5,000 = 15,000,000
90% of user profiles and role assignments are explicitly defined at the zone level	

Active Directory environment Sample #2 configuration recommendations :

SQL Server edition	SQL Server Standard Edition or above
SQL Server memory	64 GB
SQL Server disk space	80 GB

Setting the Maximum Server Memory for SQL Server

To prevent Microsoft SQL Server from consuming too much memory, you can use the following formula to determine the recommended maximum server memory:

- Reserve 4GB from the first 16GB of RAM and then 1GB from each additional 8GB of RAM for the operating system and other applications.
- Configure the remaining memory as the maximum server memory allocated for the Microsoft SQL Server buffer pool.

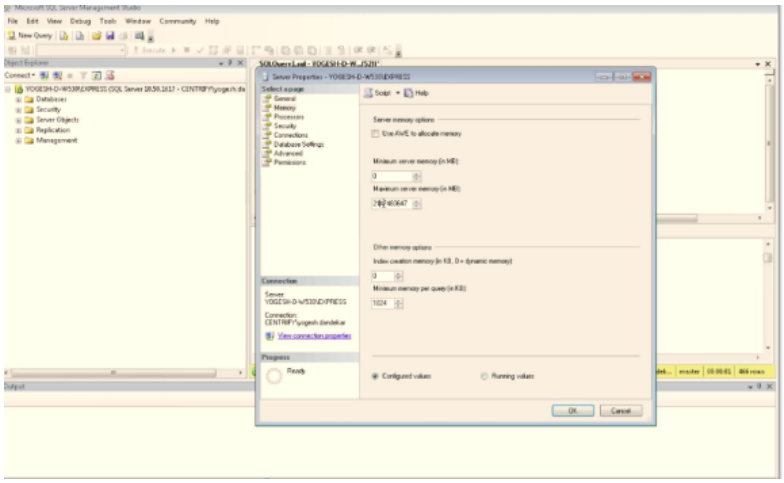
For example, if the computer hosting the Microsoft SQL Server instance has 32GB of total physical memory, you would reserve 4GB (from first 16 GB) + 1GB (from next 8 GB) + 1 GB (from next 8 GB) for the operating system, then set the Maximum server memory for Microsoft SQL Server to 26GB (32GB – 4GB – 1GB – 1GB = 26).

Reference:

https://msdn.microsoft.com/en-us/library/ms178067(v=sql.105).aspx

To set the maximum server memory for SQL Server:

1. Open the SQL Server Management Studio, enter the SQL Server properties:
2. Set the maximum server memory (in MB).



Using Report Filters to Limit the Output Data of a Report

Symptoms

In large Active Directory environments, the following reports can take too long to render because they generate a huge volume of output:

- Authorization Report
- Classic Zone – User Privileged Command Rights Report
- Classic Zone – User Role Assignment Report
- Hierarchical Zone - Computer Role Effective Assignments Report (UNIX)
- Hierarchical Zone - Computer Role Effective Assignments Report (Windows)
- Hierarchical Zone - Effective Audit Level Report
- Hierarchical Zone - Effective Rights Report
- Hierarchical Zone - Effective Role Report
- Hierarchical Zone - Users Report
- Hierarchical Zone - Zone Effective Assignments Report (UNIX)
- Hierarchical Zone - Zone Effective Assignments Report (Windows)
- All PCI reports
- All SOX reports

Resolution

You can use report filters to limit the report to only list data for specific zone types and zones in a specific domain. This can reduce the amount of data output from the report and the report will take less time to render.

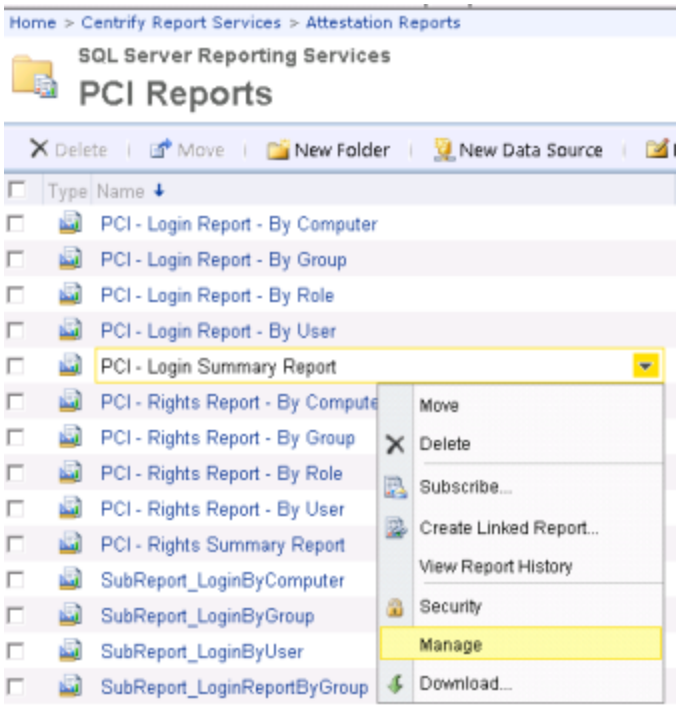
If you are opening the PCI and SOX reports, you can use the Zone Type filter to limit the reports to only list data for Classic zones or Hierarchical zones.

For all reports, you can use the Zone Domain filter to limit the reports to only list data for zones in a specific domain. By default, the Zone Domain filter of all the reports is set to the first zone domain.

By default, reports are set to run automatically when you open the report. If you prefer to set the reports to not run automatically upon opening, do the following. You must have manage report permission in order to configure the report.

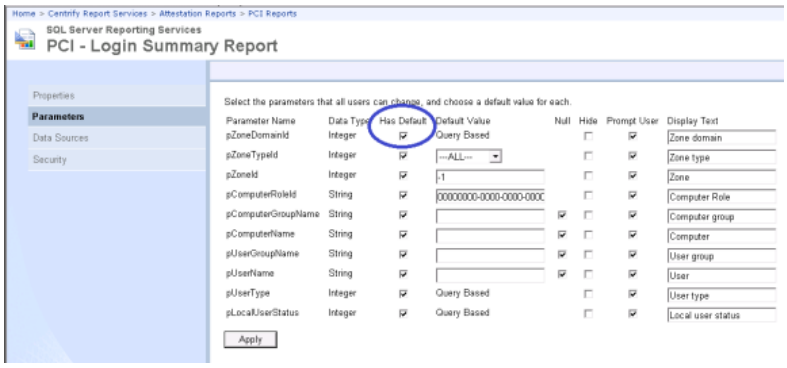
To configure a report to not run automatically when you open the report:

1. In the list of reports in the web browser, locate the desired report.
2. Move your mouse pointer over the report to open the report context menu.
3. From the context menu, select **Manage**.

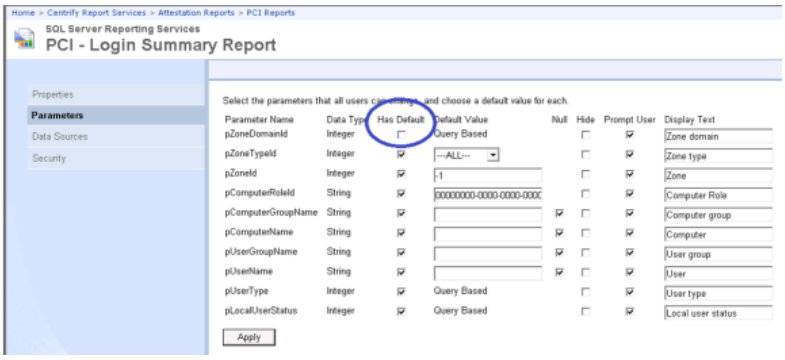


4. Select the **Parameters** page.

   Notice that 'Has Default' is selected for all parameters.

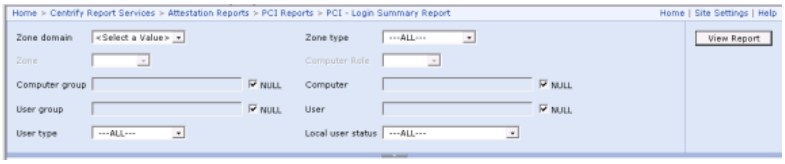


5. Deselect the ‘Has Default’ setting for any one parameter.
6. Click **Apply** to save the changes.



7. Open the report.

   The report does not run automatically. You can specify the filter values and click “View Report” button to run the report.



Increasing the Time-Out Value for Rebuild/Refresh Data Operations

Delinea Report Services invokes multiple database operations when it refreshes and rebuilds its cache of information stored in Active Directory. These database operations can be time-consuming in a large Active Directory environment. If any such database operation cannot be completed within a certain time period, the Delinea Report Services control panel will show that the Refresh/Rebuild process failed.

Symptom

When Delinea Report Services perform a snapshot rebuilding or refreshing and the amount of the monitored data is too large to be processed within the time-out period, this error will occur:

A database operation error occurred. Please contact your administrator to make sure the remote database is accessible and working properly. ---> System.Data.SqlClient.SqlException: Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding.

Resolution

You can change the time-out value (3,600 seconds by default) for that time period by performing the following steps:

1. Open the registry editor and then locate the key ‘SQLCmdTimeout’ under HKLM\Software\Centrify\Report Services\Service. If you cannot find it under the path, create one with the same name and as 'DWORD' type.

2. Set to 'SQLCmdTimeout' to a large enough value (unit in second) so that the rebuild/refresh/computing can be finished within the time period.

> Set the SQLCmdTimeout to 0 (ZERO) mean no time-out. Customer should contact Delinea Technical Support first before changing SQLCmdTimeout to 0.

Increasing the Time-Out Values for Microsoft SQL Server Reporting Services

Consider increasing the following SSRS configuration parameter values so that the large reports can be opened successfully.

Report Execution Time-out

A report execution time-out value is the maximum number of seconds that report processing can continue before it is stopped. This value is defined at the system level. You can vary this setting for individual reports.

Symptoms

For example, you can run a report that has underlying queries that cannot be completed within the time-out period. The following error will be shown on the Report Manager like this:

An error has occurred during report processing. (rsProcessingAborted)
Query execution failed for dataset 'DataSet1'. (rsErrorExecutingCommand)
A severe error occurred on the current command. The results, if any, should be discarded. Operation cancelled by user.

Resolution

Increase the Report execution time-out value. For details, see https://msdn.microsoft.com/en-us/library/ms155782.aspx.

HTTP Runtime Execution Timeout

Symptoms

You cannot open the report and you get the following error instead. This error generally occurs when the HTTP runtime execution timeout is too short.

The remote server returned an error: (500) Internal Server Error.

Resolution

1. Open the Report Server's Web.config file, which is usually in this location:

   <Drive>:\Program Files\Microsoft SQL Server\MSRS<version number>.<instance name>\Reporting Services\ReportServer

2. Locate the HttpRuntime parameter and alter the value. If it doesn't exist, you will have to create it within the section.

```
    <trace enabled="false" requestLimit="10" pageOutpu
    <sessionState mode="Off" />
    <httpHandlers>
      <add verb="*" path="Reserved.ReportServer" type=
      <add verb="*" path="Reserved.ReportViewerWebCont
Culture=neutral, PublicKeyToken=89845dcd8080cc91" />
      <add verb="GET,HEAD" path="ScriptResource.axd" t
PublicKeyToken=31bf3856ad364e35" validate="false" />
    </httpHandlers>
    <httpModules>
      <clear />
      <add name="OutputCache" type="System.Web.Caching
      <add name="WindowsAuthentication" type="System.W
      <add name="FormsAuthentication" type="System.Web
      <add name="PassportAuthentication" type="System.
      <add name="RoleManager" type="System.Web.Securit
      <add name="UrlAuthorization" type="System.Web.Se
      <add name="FileAuthorization" type="System.Web.S
      <add name="AnonymousIdentification" type="System
      <add name="Profile" type="System.Web.Profile.Pro
      <add name="ErrorHandlerModule" type="System.Web.
/>
    </httpModules>
    <globalization requestEncoding="utf-8" responseEnc
    <httpRuntime executionTimeout="9000" />
    <securityPolicy>
      <trustLevel name="RosettaSrv" policyFile="rssrvp
    </securityPolicy>
    <trust level="RosettaSrv" originUrl="" />
    <webServices>
      <soapExtensionTypes>
        <add type="Microsoft.ReportingServices.WebServ
```

The default value is 9000, and the value is in the seconds. The maximum value is 922337203685.

3. Increase the executionTimeout value to allow the report to be rendered.

Increasing the ReceiveTimeOut Value for Internet Explorer

Symptoms

The following error is shown when you try to open a report:

An unknown error occurred while processing the request on the server. The status code returned from the server was: 12002

Resolution

> The resolution for this symptom involves changing a registry setting. Before you change this registry setting, you should contact Delinea Technical Support first.

You can change the ReceiveTimeout setting for Internet Explorer using the following steps:

1. Start the Windows Registry Editor.
2. Locate the following subkey:

   HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
3. In this subkey, add a ReceiveTimeout DWORD entry that has a value of (<number of seconds>)*1000.

   For example, if you want the time-out duration to be 120 minutes, set the value of the ReceiveTimeout entry to 7200000 (<120*60>*1000).
4. Restart the computer.

Using a URL to Export Report Data to CSV

Symptoms

The underlying queries in some reports take a long time to execute and you may get the following errors when opening reports:

The remote server returned an error: (500) Internal Server Error.

Resolution

Besides using the report filters to make the report take less time to execute as described in earlier section, you can export the report to CSV by using a URL. In addition, you can skip exporting the chart data for the following reports:

- PCI – Login Summary Report
- PCI – Right Summary Report
- SOX – Login Summary Report
- SOX – Right Summary Report

To configure the report URL to export to CSV and skip the chart data in the exported file:

1. Compose the URL in the following format:

   ```
   http://\<hostname\>:\<port\>/ReportServer_\<instancename\>?\<report
   path\>&rs:Command=Render&rs:Format=CSV&pZoneDomainId=-1&SkipChartData=True
   ```

   For example:

   This is a URL to export the PCI – Login Summary report:

   ```
   http://win2012r2/ReportServer_
   CENTRIFYSUITE?%2fcentrify+Report+Services%2fAttestation+Reports%2fPCI+Reports%2fPCI+-
   +Login+Summary+Report&rs:Command=Render&rs:Format=CSV&SkipChartData=True&pZoneDomainId=-1
   ```

   This is a URL to export the PCI – Right Summary report:

   ```
   http://win2012r2/ReportServer_
   CENTRIFYSUITE?%2fcentrify+Report+Services%2fAttestation+Reports%2fPCI+Reports%2fPCI+-
   +Right+Summary+Report&rs:Command=Render&rs:Format=CSV&SkipChartData=True&pZoneDomainId=-1
   ```

2. Access the URL in Internet Explorer.
3. Save the exported CSV file.

References

https://msdn.microsoft.com/en-us//library/ms153586.aspx

https://msdn.microsoft.com/en-us/library/ms159261.aspx

Creating the Report Subscription for CSV Export

This section shows how to use the SQL Server Reporting Services (SSRS) subscription feature to export report data to CSV regularly.

Prerequisites

- Please check whether your SQL Server edition supports the reporting subscription feature. https://msdn.microsoft.com/en-us/library/cc645993(v=sql.100).aspx
- SQL Server Agent is already installed and running.

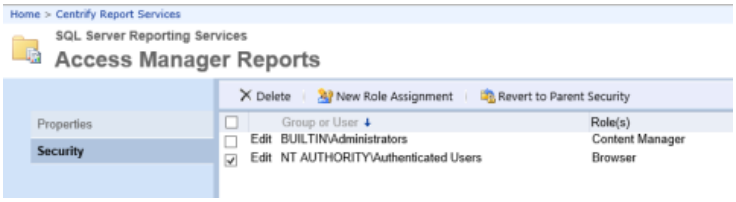
Configuring The Report Data Source For Subscriptions

To configure a report subscription in SSRS for CSV export and skip the chart data in the export:

1. Open Delinea Report Services.
2. Click **ReportDataSource** to open the report data source properties page.
3. Configure the report data source to store connection credentials in the report server:
   a. For the connection method, select **Credentials stored securely in the report server**.
   b. Enter the login user name and password.
   c. Select **Use as Windows credentials when connecting to the data source**.
   d. The following screenshot is an example of the connection settings configuration:

4. Secure access to the reports and the report data by adding or editing role assignments for the report folder.

a. Open the Security page for the report folder ‘Access Manager Reports’ and ‘Attestation Reports’.
   i. Here you can view, add, edit, or delete role assignments for the report folder.
   ii. The data source uses stored credentials, which means that users who are able to view the reports would be able to read the report data. To avoid this potential risk, you can define role-based security for reports in the Security page, as shown below.



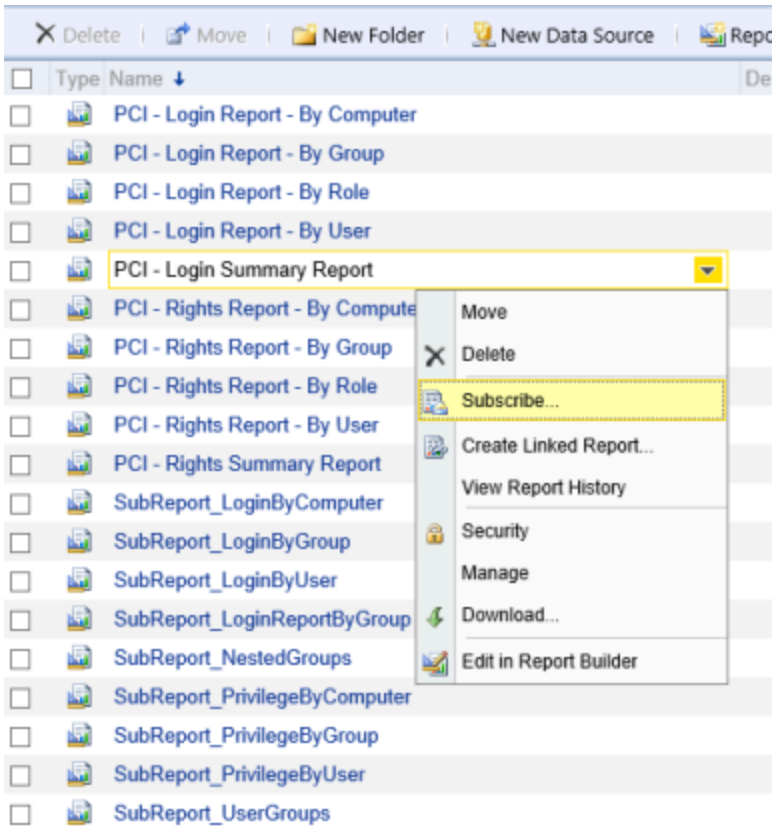
b. Delete the default role assignment that assigns the Browser role to NT AUTHORITY\Authenticated Users to remove report read access to all authenticated users.
c. In the report folder’s Security page, click New Role Assignment.
d. Enter the users or groups who can access the reports.
e. Select one or more roles to assign to the specified user(s).

   For example, if you want the specified users to only view the report, select the Browser role.
f. Click OK to save the changes.

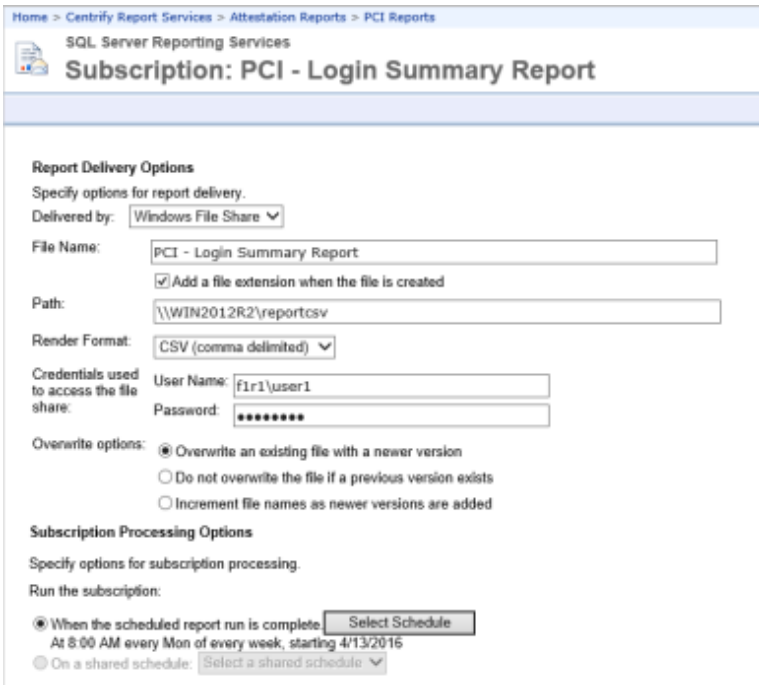
Creating A CSV Report Subscription

To configure a report subscription in SSRS for CSV export and skip the chart data in the export:

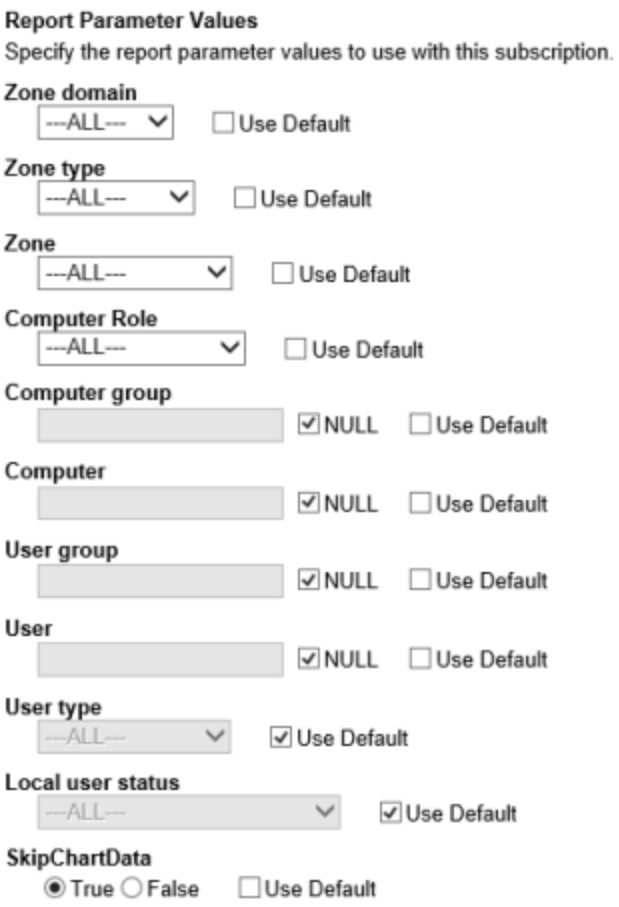
1. In the list of reports, select the report that you want to export to CSV.
2. Click the context menu and click **Subscribe**.



3. In the **Subscription** page, set the options according to the following screenshot.
   a. To specify when the scheduled report runs, click **Select Schedule**.
   b. When you specify the file path, the path must conform to the Uniform Naming Convention format.



c. In the lower area of the subscription page, set the Zone domain parameter to **ALL** in order to export report data for all zone domains.



4. After setting the options, click **OK** to create this subscription.

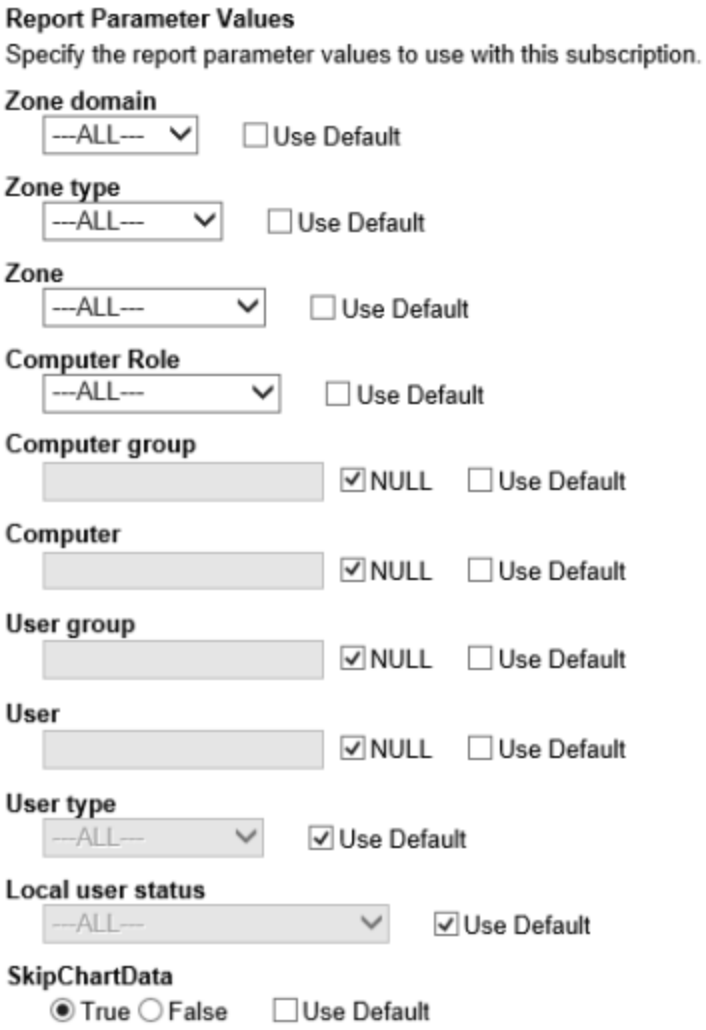
Skipping Chart Data From CSV Report Subscriptions

You can skip exporting the chart data to CSV for the following reports:

- PCI – Login Summary Report
- PCI – Right Summary Report
- SOX – Login Summary Report
- SOX – Right Summary Report

To configure a report subscription in SSRS for CSV export and skip the chart data in the export:

1. Open the report subscription. (From the report's context menu, click Manage, and then click the **Subscription** page.)
2. In the lower area of the subscription page, set the **SkipChartData** parameter to **True**.



3. After setting the options, click **OK** to save the subscription.

Views to Use in Custom Reports

Database views provide an easier and more secure way to share the reporting data without having to expose the database tables directly. Each view is essentially a database query. Some columns refer to columns in other views, and these relationships are noted.

Understanding the Differences Between Views

There are many views that are very similar to each other but provide different levels of details related to role assignments and so forth. This section briefly covers the differences between views so that you can decide which view to use, based on your needs.

When choosing which view to use, keep in mind that a view that provides less detail results in a faster query response time.

What is Included in a View	Which Views You Can Use
A list of who can log in to which computers	EffectiveAuthorizedUsers_Computer (Including computers in classic and hierarchical zones) EffectiveAuthorizedUsers_Computer_Classic (Only computers in classic zones) EffectiveAuthorizedUsers_Computer_ Hierarchical (Only computers in hierarchical zones
A list of who can log in to which computer and what privileges are granted to these users	EffectiveLoginUserPrivileges_Computer EffectiveAuthorizedUserPrivileges_Computer (Same as EffectiveLoginUserPrivileges_Computer, just to consist the naming as the other views)
A list of Active Directory users' effective role assignments	EffectiveRoleAssignment (Both hierarchical & classic zones) EffectiveRoleAssignment_Classic (Classic zones only) EffectiveRoleAssignment_Hierarchical (Hierarchical zones only)
A list of the Active Directory users' effective privileges at the computer level (The Active Directory users list in the view may not have the access right to the computer)	EffectiveRolePrivileges_Computer
A list of the Active Directory users' effective system rights at the computer level (The Active Directory users list in the view might not have the access right to the computer)	EffectiveSysRights
A list of the authorized users' privileges The list indicates if a role or right supports its accessibility to the computer	EffectiveUserPrivileges_Computer
A list of the Active Directory users' privileges at the computer role level	EffectiveUserPrivileges_ComputerRole_Unix (Assuming all computers managed by the Computer Role are UNIX) EffectiveUserPrivileges_ ComputerRole_ Windows (Assuming all computers managed by the Computer Role are Windows)
A list of the Active Directory users' privileges at the Zone level	EffectiveUserPrivileges_Zone_Unix (Assuming all computers managed by the Zone are UNIX) EffectiveUserPrivileges_Zone_Windows (Assuming all computers managed by the Zone are UNIX)

Local users	EffectiveAuthorizedLocalUsers_Computer (A local users' version to the EffectiveAuthorizedUsers_Computer) EffectiveAuthorizedLocalUserPrivileges_Computer (A Local users' version to the EffectiveLoginUserPrivileges_Computer) EffectiveLocalUsersRoleAssignment (A Local users' version to the EffectiveRoleAssignment)

ADComputers View

The ADComputers view lists all Active Directory computers for each monitored domain.

Column name	Description	Refers to
ADComputer_-Account-Enabled	1 – Active Directory computer's account is enabled, 0 – account is disabled	
ADComputer_ AccountEnabled_Desc	The display value for ADComputer_Role (Yes/No)	
ADComputer_-Canonical-Name	Active Directory computer's canonical name	
ADComputer_CnName	The Active Directory computer's common name.	
ADComputer_-Description	The description to the Active Directory computer	
ADComputer_-Dns-Host-Name	Active Directory computer's dnsHostName	
ADComputer_DomainId	The identification number of the computer's domain.	Domains.Id
ADComputer_Domain-Name	The name of the domain that the Active Directory computer belongs to.	
ADComputer_-GUID	The object GUID of the Active Directory computer	
ADComputer_Location	The Active Directory computer's location.	
ADComputer_ ManagerGUID	The hosting Active Directory computer's GUID for the user or group.	
ADComputer_ ManagerObjectName	The Active Directory computer's manager object name.	

ADComputer_ ManagerType	The type of computer manager. 1=user, 2=group.	
ADComputer_ ManagerType_Desc	The description of the Active Directory manager type.	
ADComputer_ ObjectName	The object name of the computer, in the format of <computer CN>.<computer domain>.	
ADComputer_-OS	Active Directory computer's operating system	
ADComputer_-Os-Version	Active Directory computer's operating system version	
ADComputer_OU	The OU of the Active Directory computer. It will be null if the computer is not under an OU	
ADComputer_ PwdLastChangedTime	The last changed time for Active Directory computer's password (UTC time). This is an approximation only.	
ADComputer_Role	Whether the computer is running as a domain controller or not 1 - workstation role, 2 - domain controller role	
ADComputer_Role_ Desc	The display value for ADComputer_Role (Workstation/Domain Controller)	
ADComputer_-Sam-Account-Name	Active Directory computer's samAccountName	
ADComputer_-Time-Created	The creation time of the Active Directory computer (UTC time)	
ADComputer_ TrustedDelegate	Allows services to act on behalf of another user.	

Adcomputers Columns Used in Other Views

Column name	Referred from other view
ADComputer_-GUID	ADGroupComputerMembers.ADComputer_GUID ComputerRoleMembership.ADComputer_GUID ZoneComputers.ZoneComputer_ADComputerId

ADComputers_Stale View

The ADComputers_Stale view lists all stale Active Directory computers for each domain. Computers are considered as stale if the passwords for them haven't changed for 90 or more days.

Column Name	Description	Refers to
ADComputer_ AccountEnabled	1 – Active Directory computer's account is enabled, 0 – account is disabled	
ADComputer_ AccountEnabled_Desc	The display value for ADComputer_Role (Yes/No)	
ADComputer_- Canonical-Name	Active Directory computer's canonical name	
ADComputer_CnName	The Active Directory computer's common name.	
ADComputer_- Description	The description about the Active Directory computer	
ADComputer_ DnsHostName	Active Directory computer's dnsHostName	
ADComputer_DomainId	The ID of the computer's domain	Domains.Id
ADComputer_ DomainName	The name of the domain which the Active Directory computer belongs to	
ADComputer_GUID	The object GUID of the Active Directory computer	
ADComputer_ ObjectName	The object name of the computer, in the format of <computer CN>.<computer domain>.	
ADComputer_OS	Operating system of Active Directory computer	
ADComputer_OsVersion	The operating system version number of the Active Directory computer.	
ADComputer_OU	The OU of the Active Directory computer. It will be null if the computer is not under an OU	
ADComputer_ PwdLastChangedTime	The last changed time for Active Directory computer's password (UTC time). This is an approximation only.	
ADComputer_-Role	Whether the computer is running as a domain controller or not 1 - workstation role, 2 - domain controller role	
ADComputer_Role_ Desc	The display value for ADComputer_Role (Workstation/Domain Controller)	

ADComputer_ SamAccountName	Active Directory computer's samAccountName	
ADComputer_-Time-Created	The creation time of the Active Directory computer (UTC time)	

ADGroupComputerMembers View

The ADGroupComputerMembers lists all computers that are members for each Active Directory group. Nested members are included.

Column Name	Description	Refers to
ADComputer_ CanonicalName	The canonical name of the Active Directory computer	
ADComputer_ CnName	The Active Directory computer's common name.	
ADComputer_ DnsHostName	The DNS host name of the Active Directory computer	
ADComputer_GUID	The GUID of the Active Directory computer	ADComputers.ADComputer_ GUID
ADComputer_ ObjectName	The object name of the computer, in the format of <computer CN>.<computer domain>.	
ADComputer_Os	The operating system name of the Active Directory computer	
ADComputer_ OsVersion	The OS version of the Active Directory computer	
ADComputer_ SamAccountName	The samAccountName of the Active Directory computer	
ADGroup_ CanonicalName	The canonical name of the Active Directory group	
ADGroup_GUID	The GUID of the Active Directory group	ADGroups.GUID
ADGroup_Name	The name of the Active Directory group	
ADGroup_ ObjectName	The display name for the Active Directory group, formatted as <group samAccountName>@<domain name>.	

ADGroups View

The ADGroups view lists all Active Directory groups for each domain.

Column Name	Description	Refers to
ADGroup_ ManagerGUID	The hosting Active Directory computer's GUID for the user or group.	
ADGroup_ ManagerObjectName	The object name for the user or group who manages this group.	
ADGroup_ ManagerType	The type of object that is the manager for this group. 1=user, 2=group.	
ADGroup_ ManagerType_Desc	The description of the Active Directory manager type.	
CanonicalName	Active Directory group's canonical name	
Description	Active Directory group's description	
DomainId	The identification for the domain which the Active Directory group belongs to	Domains.Id
Email	Active Directory group's email	
GroupName	Active Directory group's name	
GUID	The object GUID of the Active Directory group.	
IsBuiltIn	1 – is built in group, 0 – is not built in group	
NTLogonName	The NT logon name (samAccountName) of the Active Directory group	
ObjectName	The display name for the Active Directory group, formatted as <group samAccountName>@<domain name>.	
OU	The OU of the Active Directory group. It is null if the group is not under an OU	
TimeCreated	The creation time of the Active Directory group (UTC time)	
Type	The scope of the Active Directory group 1 - domain local, 2 - global, 3 - universal	

ADGroups columns used in other views

Column name	Referred from other view
ADGroups.GUID	ADGroupComputerMembers.ADGroup_GUID ADGroupUserMembers.ADGroup_GUID EffectiveZoneGroups.ZoneGroup_ADGroup_GUID ZoneGroups.ZoneGroup_ADGroup_GUID EffectiveUserPrivileges_Computer.Trustee_Id EffectiveUserPrivileges_ComputerRole.Trustee_Id EffectiveUserPrivileges_Zone.Trustee_Id

ADGroupSubGroups View

Lists the Active Directory group and the nested groups, including children groups and grand-children groups.

Column Name	Description	Refers to
ParentGroup_ CanonicalName	The canonical name of the parent group	
ParentGroup_DomainId	The domainID of the parent group	Domains.Id
ParentGroup_ DomainName	The domain name of the parent group	
ParentGroup_GroupType	The group type of the parent group 1-Domain local, 2-Global, 3-Universal	
ParentGroup_ GroupTypeDesc	The display value for ParentGroup_GroupType (Domain local/Global/Universal)	
ParentGroup_ NTLogonName	The NTLogonName of the parent group	
ParentGroup_ObjectName	The object name of the parent group. The general display value for the AD group in precanned report. Format:<AD group samAccountName>@<domain Name>	
ParentGroup_ ParentGroupGUID	The object GUID of the parent group	ADGroups.GUID
ParentGroup_ ParentGroupName	The name of the parent group	
SubGroup_ CanonicalName	The canonical name of the sub group	
SubGroup_DomainId	The domainIDof the sub group	Domains.Id
SubGroup_DomainName	The domain name of the sub group	

SubGroup_ EffectiveSubGroupGUID	The object GUID of the sub group	ADGroups.GUID
SubGroup_GroupName	The group name of the sub group	
SubGroup_GroupType	The group type of the sub group 1-Domain local, 2-Global, 3-Universal	
SubGroup_ GroupTypeDesc	The display value for SubGroup_GroupType (Domain local/Global/Universal)	
SubGroup_NTLogonName	The NTLogon name of the sub group Note: There is also a column with a similar name, SubGroup_NTLogoName, that will be deprecated in a future release.	
SubGroup_ObjectName	The object name of the sub group. The general display value for the AD group in precanned report. Format:<AD group samAccountName>@<domain Name>	

ADGroupUserMembers View

The ADGroupUserMembers view lists all user members for each Active Directory group. Nested members are included.

Column Name	Description	Refers to
ADGroup_ CanonicalName	The canonical name of the Active Directory group	
ADGroup_GUID	The GUID of the Active Directory group	ADGroups.GUID
ADGroup_Name	The name of the Active Directory group	
ADGroup_ ObjectName	The display name for the Active Directory group, formatted as <group samAccountName>@<domain name>.	
ADUser_GUID	The GUID of the Active Directory user	ADUsers.ADUser_ GUID
ADUser_Name	The name of the Active Directory user	
ADUser_ ObjectName	The object name for the Active Directory user.	
ADUser_ SamAccountName	The samAccountName of the Active Directory user	
ADUser_UPN	The upn name of the Active Directory user	

ADUsers View

The ADUsers view lists all Active Directory users for each monitored domain.

Column Name	Description	Refers to
ADUser_AccountExpiryDate	The expiration date for the Active Directory user account.	
ADUser_AccountLockedUntil	The date and time until which time that the user's account is locked.	
ADUser_AccountLockedUntil_Desc	The description text string for the ADUser_ AccountLockedUntil field.	
ADUser_CannotBeDelegated	Cannot be delegated.	
ADUser_CanonicalName	The canonical name of the Active Directory user	
ADUser_City	The city of the Active Directory user	
ADUser_Company	The company of the Active Directory user	
ADUser_Country	The country of the Active Directory user	
ADUser_CreationTime	The creation time of the Active Directory user	
ADUser_Department	The department of the Active Directory user	
ADUser_Description	The description of the Active Directory user	
ADUser_DialInCallbackNumber	The dialin callback number of the Active Directory user	
ADUser_DialInCallbackOptions	The dialin callback options of the Active Directory user	
ADUser_DialInCallerId	The dialin callerIDof the Active Directory user	
ADUser_DialInStaticIp	The dialin static IP address of the Active Directory user	
ADUser_DialInStaticRoutes	The dialin static routes of the Active Directory user	
ADUser_DisplayName	The display name of the Active Directory user	
ADUser_DomainId	TheIDof the Domain	Domains.Id

ADUser_DomainName	The name of the Domain	
ADUser_Email	The email of the Active Directory user	
ADUser_Enabled	If the Active Directory user account is enabled 1 - Enabled, 0 - Disabled	
ADUser_Enabled_Desc	The description string for the aduser_enabled (Yes / No)	
ADUser_FaxNumbers	The fax numbers of the Active Directory user	
ADUser_FirstName	The first name of the Active Directory user	
ADUser_GUID	The GUID of the Active Directory user	
ADUser_HomePhoneNumbers	The home phone numbers of the Active Directory user	
ADUser_Initials	The initials of the Active Directory user	
ADUser_IpPhoneNumbers	The ip phone numbers of the Active Directory user	
ADUser_IsNeverExpire	Specifies if the user account is set to never expire.	
ADUser_IsNeverExpire_Desc	The description text string for the ADUser_ IsNeverExpire column.	
ADUser_JobTitle	The job title of the Active Directory user	
ADUser_LastLogonTime	The last logon time of the Active Directory user	
ADUser_LastName	The last name of the Active Directory user	
ADUser_LogonScriptPath	The logon script path of the Active Directory user	
ADUser_ManagerGUID	The hosting Active Directory user's GUID of the user or group	
ADUser_ManagerObjectName	The Active Directory user's manager object name	
ADUser_ManagerType	The Active Directory user's manager type 1 - User, 2- Group	
ADUser_ManagerType_Desc	The Active Directory user's manager type description (User/Group)	

ADUser_MobilePhoneNumbers	The mobile phone numbers of the Active Directory user	
ADUser_Name	The name of the Active Directory user	
ADUser_ObjectName	The display name for the Active Directory user, formatted as <user samAccountName>@<domain name>.	
ADUser_Office	The office of the Active Directory user	
ADUser_PagerPhoneNumbers	The pager phone numbers of the Active Directory user	
ADUSer_PasswordNeverExpire	Password set to never expire.	
ADUser_PhoneNumbers	The phone numbers of the Active Directory user	
ADUser_PoBox	The post office box address of the Active Directory user.	
ADUser_PostalCode	The postal code (zip code) of the Active Directory user.	
ADUser_ PreauthenticationNotRequired	Pre-authentication not required.	
ADUser_PrimaryGroupId	The primary group ID of the Active Directory group.	
ADUser_ProfileHomeFolder	The profile home folder of the Active Directory user	
ADUser_ProfilePath	The profile path of the Active Directory user	
ADUser_PwdLastSetTime	The password last set time of the Active Directory user. This is an approximation only.	
ADUser_ PwdStoreUsingReversibleEncryption	Password stored using reversible encryption.	
ADUser_RemoteAccessPermissions	The remote access permissions of the Active Directory user	
ADUser_SamAccountName	The samAccountName of the Active Directory user	
ADUser_SmartCardNeededForLogon	Smart card needed for login.	
ADUser_State	The state of the Active Directory user	

ADUSer_Street	The Active Directory user's street address.	
ADUser_TrustedForDelegation	Trusted for delegation.	
ADUser_Upn	The upn name of the Active Directory user	
ADUser_UseDesEncryption	Uses DES Encryption.	
ADUser_WebPages	The web pages of the Active Directory user	

ADUser Columns Used in Other Views

Column name	Referred from other view
ADUsers.ADUser_GUID	ADGroupUserMembers.ADUser_GUID EffectiveUserPrivileges_Computer.ADUser_GUID EffectiveUserPrivileges_ComputerRole.ADUser_GUID EffectiveUserPrivileges_Zone.ADUser_GUID EffectiveZoneUsers.ZoneUser_ADUserGUID ZoneUsers.ZoneUser_ADUserGUID EffectiveUserPrivileges_Computer.Trustee_Id EffectiveUserPrivileges_ComputerRole.Trustee_Id EffectiveUserPrivileges_Zone.Trustee_Id

ApplicationRight View

The ApplicationRight view lists the detailed attributes for each application right.

Column Name	Description	Refers to
Right_Description	The description of the application right	
Right_FullName	The full name of the right <right name>/<zone name>	
Right_GUID	The GUID of the Right	Rights.Right_GUID
Right_Name	The name of the application right	
Right_Priority	The priority of the application right	
Right_RequireAuthentication	If this right requires authentication 1 - Yes, 0 - No	
Right_RequireAuthentication_Desc	If this right requires authentication (Yes/No)	
Right_RunasUser	Run as the specified AD user	

Right_ZoneId	The Id of the Zone that the Right belongs to	Zones.Zone_Id
Right_ZoneName	The name of the Zone that the Right belongs to	

AutoZoneComputers View

The AutoZoneComputers view lists the computers that are joined to the AutoZone.

Column Name	Description	Refers to
ZoneComputer_ ADComputerCnName	AD computer's cn name	
ZoneComputer_ ADComputerId	The GUID of the AD computer	ADComputers_ ADComputer_GUID
ZoneComputer_ ADComputerName	AD computer's name	
ZoneComputer_ ADComputerObjectName	Format: <AD computer CN>.<AD computer domain> Mainly used by precanned-report	
ZoneComputer_ AgentVersion	The agent version of the Auto Zone Computer	
ZoneComputer_ ComputerType	The IDof the computer type of the Auto Zone Computer. This value is always 2	
ZoneComputer_ ComputerType_Desc	The computer type of the Auto Zone Computer. This value is always 'Unix'	
ZoneComputer_Id	The ID of the Auto Zone Computer	
ZoneComputer_IsOrphan	To identifier if this is an orphan Auto Zone Computer 1 - Yes, 0 - No	
ZoneComputer_IsOrphan_ Desc	(Yes/No)	
ZoneComputer_Name	The name of the Auto Zone Computer	
ZoneComputer_ZoneId	The ID of the zone. Always be -1	
ZoneComputer_ZoneName	The name of the zone. The value is always 'Auto Zone'	

CommandRight View

This view lists the detailed attributes for each command right.

Column Name	Description	Refers to
Right_AddVar	Comma separated list of environment variable name-value pairs to add	
Right_AllowNested	Nested command execution is allowed or not 1 – Yes, 0 – No	
Right_AllowNested_Desc	The description to the Right_AllowNested (Yes/No)	
Right_Authentication	Type of authentication required to run the command	
Right_DeleteVar	Comma separated list of environment variables to delete in addition to the default set	
Right_Description	The description of the command right	
Right_DzdoRunAsGroup	Comma separated list of groups allowed to run this command using dzdo	
Right_DzdoRunAsUser	Comma separated list of users, uids, groups or gids allowed to run this command using dzdo	
Right_DzshRunas	The user this command will run as under dzsh	
Right_FullName	The full name of the command rights. Format <command right name>/<zone name>	
Right_GUID	The GUID of the command right	Rights.Right_GUID
Right_KeepVar	Comma separated list of environment variables to keep in addition to the default set	
Right_MatchPath	The match path of the command right	
Right_Name	The name of the command right	
Right_Pattern	The pattern of the command right	
Right_PatternType	The type of the command right pattern 0 – Global, 1 – Regular expression	
Right_PatternType_Desc	The description of the type of the command right pattern (Global / Regular expression)	

Right_ PreserveGroup	Preserve group membership or not	
Right_Priority	The priority of the command right	
Right_UMask	The umask value used to define who can execute the command	
Right_ZoneId	The ID of the zone that the command right is defined	Zones.Zone_Id
Right_ZoneName	The name of the zone that the command right is defined	

ComputerRoleCustomAttribute View

This view lists the computer role custom attributes.

Column Name	Description	Refers to
RoleAssignment_GUID	The computer role's object GUID.	ComputerRoles.ComputerRole_GUID
CustomAttribute_Name	The custom attribute's name.	
CustomAttribute_Value	The custom attribute's value.	

ComputerRoleEffectiveMembers View

This view lists the effective members of a computer role.

Column Name	Description	Refers to
ComputerRole_GUID	The GUID of the Computer Role	
ComputerRole_ZoneId	The zone ID where the Computer Role is defined	Zones.Zone_Id
ComputerRole_ ComputerRoleName	The name of the Computer Role	
ADComputer_GUID	The object GUID of the Active Directory computer	ADComputes.ADComputer_ GUID
ADComputer_ DomainId	The ID of the computer's domain	Domains.Id
ADComputer_ ObjectName	Format: <AD computer CN>.<AD computer domain> This field is mainly used by the default reports.	

ADComputer_ CnName	The Active Directory computer's cnName	
ADComputer_ DnsHostName	The DNS host name of the Active Directory computer	
ZoneComputer_Id	The ID of the computer	
ZoneComputer_ ZoneId	The ID of the zone that the computer is managed by	Zones.Zone_Id
ZoneComputer_Name	The name of the computer	
ZoneComputer_ AgentVersion	The agent version of the computer	
ZoneComputer_ Platform	The platform of the computer 1 – Windows, 2 – UNIX	
ZoneComputer_ Platform_Desc	The description string of the ZoneComputer_ Platform (Windows/UNIX)	
ZoneComputer_ IsOrphan	If the computer is orphan 1 – Yes, 0 – No	
ZoneComputer_ JoinDate	The date when the computer joined zone (UTC time)	

ComputerRoleMembership View

The ComputerRoleMembership view lists all computer members for each Computer Role. The view includes computers that have been added into the zone.

Column Name	Description	Refers to
ADComputer_CnName	The Active Directory computer's common name.	
ADComputer_ DnsHostName	The dns host name of the Active Directory Computer	
ADComputer_DomainId	The domain ID of the Active Directory computer	Domains.Id
ADComputer_GUID	The GUID of the Active Directory computer	ADComputes.ADComputer_ GUID

ADComputer_ ObjectName	The object name of the computer, in the format of <computer CN>.<computer domain>.	
ComputerRole_ ComputerRoleName	The name of the Computer Role	
ComputerRole_GUID	The object GUID of the computer role	
ComputerRole_ZoneId	The ID of the zone where this computer role is defined	Zones.Zone_Id
ZoneComputer_ AgentVersion	The agent version of the computer	
ZoneComputer_Id	The ID of the computer	
ZoneComputer_ IsOrphan	If the computer is orphaned 1 - Yes, 0 - No	
ZoneComputer_ JoinDate	The date when the computer joined zone (UTC time)	
ZoneComputer_Name	The name of the computer	
ZoneComputer_ Platform	The computer platform 1 - Windows, 2 - Unix	
ZoneComputer_ PlatformDesc	The display value of ZoneComputer_Platform (Windows/Unix)	
ZoneComputer_ZoneId	The ID of the zone where the computer is joined to	Zones.Zone_Id

ComputerRoles View

This view lists the computer role information.

Column Name	Description	Refers to
ComputerRole_ Description	The description of the Computr Role	
ComputerRole_ GroupGUID	The GUID of the AD group which the Computer Role monitoring	ADGroups.GUID
ComputerRole_ GroupName	The name of the AD group which the Computer Role monitoring	

ComputerRole_GUID	The GUID of the Computer Role	
ComputerRole_Name	The name of the Computer Role	
ComputerRole_ZoneId	The ID of the zone where the Computer Role is defined	Zones.Zone_Id
ComputerRole_ZoneName	The name of the zone where the Computer Role is defined	

DelegationTasks View

This view lists which user, group, computer, or well-known SID have which delegation tasks.

Column Name	Description	Refers to
Target	The target in which the Server Suite task is delegated	
Target_ DomainId	The domain ID of the target	Domains.Id
Target_ GUID	The GUID of the target	
Zone_Id	The zone ID	Zones.Zone_Id
Scope	The scope in which the Server Suite task is delegated	
Scope_Id	The scope ID: 1 - Zone; 2 - UNIX Computer; 3 - WINDOWS Computer; 4 - Computer Role	
Trustee_ Name	The trustee name	
Trustee_ Type	The trustee type is one of the following: 1 - User; 2 - UNIX computer; 3 - Windows computer; 4 - computer role.	
Trustee_ Type_Desc	The description of the trustee type	
Trustee_ DomainId	The domain ID of the trustee	Domains.Id
Task_Id	Task Id	DelegationTaskType.Task_Id
Task_Name	Task name	

DelegationTaskType View

This view lists the Server Suite delegation tasks.

Column Name	Description	Refers to
Task_Name	Task name	
Task_Id	Task Id	

Domains View

The Domains view lists all monitored domains.

Column Name	Description
Dc	The domain controller for the monitored domain
DomainName	The name of the monitored domain
Id	The ID of the monitored domain

Domains Columns Used in Other Views

Column name	Referred from other view
Domains.Id	ADComputers.ADComputer_DomainID ADComputers_Stale.ADComputer_DomainId ADGroups.DomainId ADUsers.ADUser_DomainID ComputerRoleMembership.ADComputer_DomainId RoleAssignments_ComputerRole.RoleAssignment_ZoneDomainId UserAccounts.ADUser_DomainId ZoneRolePrivileges.ZoneRolePrivileges_RightZoneDomainId Zones.Zone_DomainID Zones_Classic.Zone_DomainID Zones_Hierarchical.Zone_DomainID

EffectiveAuthorizedUserPrivilegesSummary View

This view lists effective privileges rights granted to Active Directory users for both hierarchical and classic zones.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the Active Directory user that the user profile refers to.	ADUsers.ADUser_GUID
ZoneComputer_ID	The object GUID ID of the computer profile	ZoneComputers. ZoneComputer_Id

Right_GUID	The GUID of the right	Rights.Right_GUID

EffectiveAuthorizedUserPrivilegesSummary__Hierarchical View

This view lists effective privileges rights granted to Active Directory users for just hierarchical zones.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the Active Directory user that the user profile refers to.	ADUsers.ADUser_GUID
ZoneComputer_ID	The object GUID ID of the computer profile	ZoneComputers. ZoneComputer_Id
Right_GUID	The GUID of the right	Rights.Right_GUID

EffectiveAuthorizedUserPrivilegesSummary_Classic View

This view lists effective privileges rights granted to Active Directory users for just classic zones.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the Active Directory user that the user profile refers to.	ADUsers.ADUser_GUID
ZoneComputer_ID	The object GUID ID of the computer profile	ZoneComputers. ZoneComputer_Id
Right_GUID	The GUID of the right	Rights.Right_GUID

EffectiveAuthorizedLocalUserPrivileges_Computer View

This view lists the authorized local user's effective rights and privileges for each computer.

Column Name	Description	Refers to
ADComputer_ CanonicalName	The canonical name of the Active Directory computer	
ADComputer_ CnName	The cn name of the Active Directory computer	
ADComputer_ DnsHostName	The dns host name of the Active Directory computer	

ADComputer_ ObjectName	The object name of the Active Directory computer	
Assigned_Location	The display value of the source assignment location	
Assigned_ LocationType	The source assignment location	
Assigned_ LocationType_Desc	The type of the source assignment location 1 – Zone 2 – Computer 3 – Computer Role	
EffectiveZone_Id	The auto generated ID of the Zone	Zones.Zone_Id
EffectiveZone_ Name	The name of the Zone	
LocalUser_Name	The name of the local user	
LocalUser_ ProfileState	The profile state of the local user 1 =Enabled, 2 = Disabled, 3 = Removed from /etc/passwd	
LocalUser_ ProfileState_Desc	The display value for LocalUser _ProfileState (Enabled/Disabled/Removed from /etc/passwd)	
Right_FullName	The full name of the right. Format in <Right name> / <Right's zone name>	
Right_Grants_ Logon	If this right could support a user to logon to a system 1 – Yes, 0 – No	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	The ID of the right platform	
Right_Platform_ Desc	The display value of the right platform	
Right_Type	The type ID of the right	RightType.RightTypeId
Right_Type_Desc	The type description of the right	
Role_FullName	The full name of the role. Format in <Role name> / <Role's zone name>	

Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
Trustee_Name	The trustee name of the role assignment	
Trustee_Type	The trustee type ID of the role assignment	TrusteeTypes.TrusteeType_Id
Trustee_Type_ Desc	The type description of the trustee	
ZoneComputer_Id	The object GUID ID of the computer profile	ZoneComputers. ZoneComputer_Id

EffectiveAuthorizedLocalUsers_Computer View

This view lists the effective, authorized local users for each computer.

Column Name	Description	Refers to
LocalUser_Name	The name of the local user	ZoneLocalUsers.ZoneLocalUser_ Name
ZoneComputer_Id	The ID of the zone computer	ZoneComputers.ZoneComputer_Id
LocalUserProfileState	The state of the local user profile, indicated by a number: Enabled Disabled Removed from /etc/passwd	
LocalUser_ ProfileState_Desc	The text description of LocalUserProfileState	

EffectiveAuthorizedUserPrivileges_Computer View

This view lists the users who are authorized to log in and the computers that they can log in to. This EffectiveAuthorizedUserPrivileges_Computer view is the same as EffectiveLoginUserPrivilege_Computer View .

EffectiveAuthorizedUsers_Computer View

This view lists the users who can log in and the computers that they can log in to.

Column Name	Description	Refers to

ADUser_GUID	The object GUID of the Active Directory user that the user profile refers to.	ADUsers.ADUser_GUID
ZoneComputer_Id	The computer profile's object GUID.	ZoneComputer.ZoneComputer_ID

EffectiveAuthorizedUsers_Computer_Classic View

This view lists the users who can log in and the classic zone computers that they can log in to.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the Active Directory user that the user profile refers to.	ADUsers.ADUser_GUID
ZoneComputer_Id	The computer profile's object GUID.	ZoneComputer.ZoneComputer_ID

EffectiveAuthorizedUsers_Computer_Hierarchical View

This view lists the users who can log in the hierarchical zone computers that they can log in to.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the Active Directory user that the user profile refers to.	ADUsers.ADUser_GUID
ZoneComputer_Id	The computer profile's object GUID.	ZoneComputer.ZoneComputer_ID

EffectiveAuthorizedZoneLocalUsers View

This view lists the effective user profiles for local users who can log in and the computers that they can log in to.

Column Name	Description	Refers to
EffectiveZone_Id	The auto generated ID of the Zone	Zones.Zone_Id
EffectiveZone_Name	The name of the Zone	
EffectiveZone_DomainId	The domain ID of the Zone	
ZoneLocalUser_Id	The auto generated ID of the local user profile	ZoneLocalUsers. ZoneLocalUser_Id
ZoneLocalUser_Name	The name of the local user profile	

ZoneLocalUser_ HomeDirectory	The home directory of the local user profile	
ZoneLocalUser_ PrimaryGroupId	The primary group ID of the local user profile	
ZoneLocalUser_ PrimaryGroupName	The primary group name of the local user profile	
ZoneLocalUser_Shell	The shell of the local user profile	
ZoneLocalUser_Uid	The UID of the local user profile	
ZoneLocalUser_GECOS	The GECOS of the local user profile	
ZoneLocalUser_ ProfileState	The profile state of the local user profile 1 means Enabled, 2 means Disabled, 3 means Removed from /etc/passwd	
ZoneLocalUser_ ProfileState_Desc	The display value for ZoneLocalUser_ProfileState (Enabled/Disabled/Removed from /etc/passwd)	
ZoneLocalUser_ AssignmentLocation_ Type	The type code of the location where the zoned local user is assigned	
ZoneLocalUser_ AssignmentLocation_ Type_Desc	The display text of the type of the location where the zoned local user is assigned	
ZoneLocalUser_ AssignmentLocation_ GUID	The GUID of the location object where the zoned local user is assigned	
ZoneLocalUser_ AssignmentLocation_ Name	The name of the location object where the zoned local user is assigned	
ZoneComputer_Id	The object GUID of the computer profile	ZoneComputers. ZoneComputer_Id
ADComputer_ ObjectName	The object name of the ad computer	
ADComputer_ DnsHostName	The DNS host name of the ad computer	

ADComputer_CnName	The CN name of the ad computer	
ADComputer_Os	The operating system of the Active Directory computer	
ADComputer_DomainId	The domain ID of the Active Directory computer	

EffectiveAuthorizedZoneUsers View

This view lists the authorized Active Directory user's effective user profiles for each computer.

Column Name	Description	Refers to
EffectiveZone_Id	The auto-generated ID of the Zone	Zones.Zone_Id
EffectiveZone_Name	The name of the Zone	
EffectiveZone_DomainId	The domain ID of the Zone	
ZoneUser_Id	The auto generated ID of the user profile	ZoneUsers. ZoneUser_ Id
ZoneUser_Name	The name of the user profile	
ZoneUser_HomeDirectory	The home directory of the user profile	
ZoneUser_PrimaryGroupId	The primary group ID of the user profile	
ZoneUser_ PrimaryGroupName	The primary group name of the user profile	
ZoneUser_Shell	The shell of the user profile	
ZoneUser_Uid	The UID of the user profile	
ZoneUser_GECOS	The GECOS of the user profile	
ZoneUser_IsSecondaryProfile	Whether the user profile is a secondary profile or not: 1 – Yes 0 – No	
ZoneUser_ IsSecondaryProfile_Desc	The display value for ZoneUser_IsSecondaryProfile (Yes/No)	
ZoneUser_ AssignmentLocation_Type	The type code of the location where the zoned user is assigned	

ZoneUser_ AssignmentLocation_Type_ Desc	The display text of the type of the location where the zoned user is assigned	
ZoneUser_ AssignmentLocation_GUID	The GUID of the location object where the zoned user is assigned	
ZoneUser_ AssignmentLocation_Name	The name of the location object where the zoned user is assigned	
ADUser_DomainId	The domain ID of the Active Directory user	
ADUser_GUID	The GUID of the ad user	
ADUser_ObjectName	The object name of the Active Directory user	
ZoneComputer_Id	The object GUID ID of the computer profile	ZoneComputers. ZoneComputer_Id
ADComputer_ObjectName	The object name of the Active Directory computer	
ADComputer_DnsHostName	The DNS host name of the Active Directory computer	
ADComputer_CnName	The CN name of the Active Directory computer	
ADComputer_Os	The operating system of the Active Directory computer	
ADComputer_DomainId	The domain ID of the Active Directory computer	

EffectiveDelegationTasks View

This view lists which Active Directory user has which delegation tasks.

Column Name	Description	Refers to
Target	The target in which the Server Suite task is delegated	
Target_ DomainId	The domain ID of the target	Domains.Id
Target_GUID	The GUID of the target	
Zone_Id	The zone ID	Zones.Zone_Id

Scope	The scope in which the Server Suite task is delegated	
Scope_Id	The scope ID: 1 - Zone; 2 - UNIX Computer; 3 - WINDOWS Computer; 4 - Computer Role	
Trustee_ Name	The trustee name	
Trustee_ GUID	The GUID of trustee	
Trustee_ DomainId	The domain ID of the trustee	Domains.Id
Task_Id	Task Id	DelegationTaskType.Task_Id
Task_Name	Task name	

EffectiveGroupPrivileges_Computer View

This view lists the consolidated role assignments, logon privileges, system rights privileges for each group and computer. This view only lists the role assignments that are assigned to Active Directory groups, and lists the trustee Active Directory groups and nested groups.

Column Name	Description	Refers to
ADComputer_ CanonicalName	The canonical name of the Active Directory Computer in where the privileges effective	
ADComputer_ CnName	The CN name of the Active Directory Computer in where the privileges effective	
ADComputer_ DnsHostName	The DNS host name of the Active Directory Computer in where the privileges effective	
ADComputer_ ObjectName	The object name of the Active Directory Computer in where the privileges effective	
ADGroup_ CanonicalName	The canonical name of the effective assigned Active Directory group	
ADGroup_GUID	The GUID of the effective assigned Active Directory group	ADGroups.GUID
ADGroup_Name	The name of the effective assigned Active Directory group	

ADGroup_ ObjectName	The object name of the effective assigned Active Directory group. The format is <samAccountName>@<domain name>	
ADGroup_ SamAccountName	The samAccountName of the effective assigned Active Directory group	
Assigned_Location	The name of the assignment location	
Assigned_ LocationType	The type of the assignment location 1 – Zone, 2 – Computer, 3 – Computer Role	
Assigned_ LocationTypeDesc	The description fo the type of the assignment location (Zone, Computer, Computer Role)	
Computer_Platform	The platform ID of the Active Directory Computer in where the privileges effective 1 – Windows, 2 – UNIX	
Computer_Platform_ Desc	The platform description name of the Active Directory Computer in where the privileges effective (Windows/UNIX)	
EffectiveZone_Id	The ID of the effective zone for the privilege assignment	Zones.Zone_Id
EffectiveZone_Name	The name of the effective zone for the privilege assignment	
Right_FullName	The full name of the right	
Right_Grants_Logon	If this right could support a user to logon to a system 1 – Yes, 0 – No	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	The platform ID of the right 0 – Windows, 1 – UNIX, 2 – Windows/UNIX	
Right_Platform_ Desc	The platform description of the right (Windows, UNIX, Windows/UNIX)	
Right_Type	The type ID of the right	RightType.RightTypeId

Right_Type_Desc	The type description of the right	
Role_FullName	The full name of the role <role name>/<zone name>	
Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
Trustee_Id	The GUID of the Trustee	ADGroups.ADGroup_GUID
Trustee_Name	The name of the trustee	
Trustee_Type	The type ID of the trustee type	TrusteeTypes.TrusteeType_Id
Trustee_Type_Desc	The type description of the trustee type	
ZoneComputer_Id	The ID of the Zone Computer in where the privileges effective	ZoneComputer.ZoneComputer_Id

EffectiveLocalUserPrivilegesSummary View

This view lists effective privileges rights granted to local UNIX users for both hierarchical and classic zones.

Column Name	Description	Refers to
LocalUser_Name	The name of the local user	ZoneLocalUsers.ZoneLocalUser_ Name
LocalUser_ ProfileState	The state of the local user profile, indicated by number: Enabled Disabled Removed from /etc/passwd	
LocalUser_ ProfileState_Desc	The text description of LocalUser_ProfileState.	
ZoneComputer_Id	The object GUID ID of the computer profile	ZoneComputers. ZoneComputer_Id
Right_GUID	The GUID of the right	Rights.Right_GUID

EffectiveLocalUsersRoleAssignment View

This view lists the effective role assignments for local users for each computer.

Column Name	Description	Refers to
Assigned_Location	The name of the assigned location	
Assigned_ LocationTypeDesc	The assigned location: zone, computer, or computer role	
LocalUser_Name	The name of the local user	ZoneLocalUsers.ZoneLocalUser_ Name
LocalUser_ ProfileState	The state of the local user profile, indicated by number: Enabled Disabled Removed from /etc/passwd	
LocalUser_ ProfileState_Desc	The text description of LocalUser_ProfileState.	
Role_GUID	The GUID for the role.	Roles.Role_Id
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
Trustee_Name	The trustee name	
Trustee_Type	The type of trustee, indicated by number: Active Directory user Active Directory group Local UNIX user Local UNIX group Local Windows user Local Windows group All Active Directory users All local UNIX users All local Windows users local UNIX UID	
Trustee_Type_Desc	The text description of the Trustee_Type	
ZoneComputer_Id	The ID of the zone computer.	ZoneComputers.ZoneComputer_Id

EffectiveLoginUserPrivilege_Computer View

This view lists the users who can log in and the computers that they can log in to. .

Column Name	Description	Refers to

ADComputer_ CanonicalName	The canonical name of the AD Computer in where the privileges effective	
ADComputer_ CnName	The Cn name of the AD Computer in where the privileges effective	
ADComputer_ DnsHostName	The dns host name of the AD Computer in where the privileges effective	
ADComputer_ ObjectName	The object name of the AD Computer in where the privileges effective	
ADUser_ CanonicalName	The canonical name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_FullName	The full name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_GUID	The GUID of the assigned Active Directory user. It will be null when trustee type = 7	ADUsers.ADUser_GUID
ADUser_Name	The name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_ ObjectName	The display name for the Active Directory user, formatted as <user samAccountName>@<domain name>.	
ADUser_ SamAccountName	The samAccount name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_Upn	The upn name of the assigned Active Directory user. It will be null when trustee type = 7	
Assigned_Location	The name of the assignment location	
Assigned_ LocationType	The type of the assignment location 1 – Zone, 2 – Computer, 3 – Computer Role	
Assigned_ LocationTypeDesc	The description fo the type of the assignment location (Zone, Computer, Computer Role)	
EffectiveZone_Id	The ID of the effective zone for the privilege assignment	Zones.Zone_Id

EffectiveZone_Name	The name of the effective zone for the privilege assignment	
Right_FullName	The full name of the right	
Right_Grants_Logon	If this right could support a user to logon to a system 1 – Yes, 0 – No	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	The platform ID of the right 0 – Windows, 1 – UNIX, 2 – Windows/UNIX	
Right_Platform_ Desc	The platform description of the right (Windows, UNIX, Windows/UNIX)	
Right_Type	The type ID of the right	RightType.RightTypeId
Right_Type_Desc	The type description of the right	
Role_FullName	The full name of the role <role name>/<zone name>	
Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
Trustee_ID	The ID of the Trustee	Trustee_Type = 1: ADUsers.ADUser_ GUID Trustee_Type = 2: ADGroups.ADGroup_GUID
Trustee_Name	The name of the trustee	
Trustee_Type	The type ID of the trustee type	TrusteeTypes.TrusteeType_Id
Trustee_Type_Desc	The type description of the trustee type	
ZoneComputer_Id	The ID of the Zone Computer in where the privileges effective	ZoneComputer.ZoneComputer_Id

EffectiveRoleAssignment View

This view lists all effective role assignments for each user and for each computer.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the AD user which the user profile referring to.	ADUsers.ADUser_GUID
Assigned_Location	The source assignment location	
Assigned_ LocationType	The type of the source assignment location 1 - Zone 2 - Computer 3 - Computer Role	
Assigned_ LocationType_Desc	The display value of the source assignment location	
Role_GUID	The object GUID ID of the role	Roles.Role_Id
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
Trustee_Id	The trustee ID of the role assignment	
Trustee_Name	The trustee name of the role assignment	
Trustee_Type	The trustee type ID of the role assignment	TrusteeTypes.TrusteType_Id
Trustee_Type_Desc	The type description of the trustee	
ZoneComputer_Id	The object GUID ID of the computer profile	ZoneComputer.ZoneComputer_Id

EffectiveRoleAssignment_Classic View

This view lists all effective role assignments in classic zones for each user and for each computer.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the AD user which the user profile referring to.	ADUsers.ADUser_GUID
Assigned_Location	The source assignment location	
Assigned_ LocationType	The type of the source assignment location 1 - Zone 2 - Computer 3 - Computer Role	

Assigned_ LocationType_Desc	The display value of the source assignment location	
Role_GUID	The object GUID ID of the role	Roles.Role_Id
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
Trustee_Id	The trustee ID of the role assignment	
Trustee_Name	The trustee name of the role assignment	
Trustee_Type	The trustee type ID of the role assignment	TrusteeTypes.TrusteType_Id
Trustee_Type_Desc	The type description of the trustee	
ZoneComputer_Id	The object GUID ID of the computer profile	ZoneComputer.ZoneComputer_Id

EffectiveRoleAssignment_Hierarchical View

This view lists all effective role assignments in hierarchical zones for each user and for each computer.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the AD user which the user profile referring to.	ADUsers.ADUser_GUID
Assigned_Location	The source assignment location	
Assigned_ LocationType	The type of the source assignment location 1 - Zone 2 - Computer 3 - Computer Role	
Assigned_ LocationType_Desc	The display value of the source assignment location	
Role_GUID	The object GUID ID of the role	Roles.Role_Id
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID

RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
Trustee_Id	The trustee ID of the role assignment	
Trustee_Name	The trustee name of the role assignment	
Trustee_Type	The trustee type ID of the role assignment	TrusteeTypes.TrusteType_Id
Trustee_Type_Desc	The type description of the trustee	
ZoneComputer_Id	The object GUID ID of the computer profile	ZoneComputer.ZoneComputer_Id

EffectiveRolePrivileges_Computer View

This view lists the consolidated role assignments, logon privileges, system rights privileges for each computer. This view does not expand the trustee to individual Active Directory users.

Column Name	Description	Refers to
ADComputer_ CanonicalName	The canonical name of the AD Computer in where the privileges effective	
ADComputer_ CnName	The Cn name of the AD Computer in where the privileges effective	
ADComputer_ DnsHostName	The dns host name of the AD Computer in where the privileges effective	
ADComputer_ ObjectName	The object name of the AD Computer in where the privileges effective	
Assigned_Location	The name of the assignment location	
Assigned_ LocationType	The type of the assignment location 1 – Zone, 2 – Computer, 3 – Computer Role	
Assigned_ LocationTypeDesc	The description fo the type of the assignment location (Zone, Computer, Computer Role)	
Computer_Platform	The platform ID of the AD Computer in where the privileges effective 1 – Windows, 2 – UNIX	

Computer_Platform_Desc	The platform description name of the AD Computer in where the privileges effective (Windows/UNIX)	
EffectiveZone_Id	The ID of the effective zone for the privilege assignment	Zones.Zone_Id
EffectiveZone_Name	The name of the effective zone for the privilege assignment	
Right_Description	The description of the right.	
Right_FullName	The full name of the right	
Right_Grants_Logon	If this right could support a user to logon to a system 1 – Yes, 0 – No	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	The platform ID of the right 0 – Windows, 1 – UNIX, 2 – Windows/UNIX	
Right_Platform_Desc	The platform description of the right (Windows, UNIX, Windows/UNIX)	
Right_Type	The type ID of the right	RightType.RightTypeId
Right_Type_Desc	The type description of the right	
Role_FullName	The full name of the role <role name>/<zone name>	
Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	
RoleAssignment_GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_GUID
Trustee_GUID	The GUID of the Trustee	Trustee_Type = 1: ADUsers.ADUser_GUID Trustee_Type = 2: ADGroups.ADGroup_GUID
Trustee_Name	The name of the trustee	

Trustee_Type	The type ID of the trustee type	TrusteeTypes.TrusteeType_Id
Trustee_Type_Desc	The type description of the trustee type	
ZoneComputer_Id	The ID of the Zone Computer in where the privileges effective	ZoneComputer.ZoneComputer_Id

EffectiveSysRights View

This view lists the effective system rights in hierarchical zones for each user and for each computer.

Column Name	Description	Refers to
ADUser_GUID	The object GUID of the AD user which the user profile referring to.	ADUsers.ADUser_GUID
ZoneComputer_Id	The object GUID ID of the computer profile	ZoneComputer.ZoneComputer_Id
-Audit-Level	The role's audit level (It will be null for classic zone's role) 0 – audit not required, 1 – audit if possible, 2 – audit required	
AuditLevel_Desc	The display value of Role_AuditLevel (It will be null for classic zone's role) (Audit not Required/Audit if Possible/Audit required)	
Always-Permit-Logon	(It will be null for classic zone's role) 1 – always permit, 0 – not always permit	
AlwaysPermitLogon_Desc	The display value of -Always-Permit-Logon (It will be null for classic zone's role) (Always permit/Not always permit)	
AllowPasswordLogon	Allow Password Logon 0 – No, 1 – Yes, Null – N/A	
AllowPasswordLogon_Desc	The display value of AllowPasswordLogon (No, Yes, N/A)	
AllowPsRemoteAccess	Allow PowerShell remote access 0 - No, 1- Yes, Null - N/A	
AllowPsRemoteAccess_ Desc	The display value of AllowPsRemoteAccess (No, Yes, N/A)	

AllowNonPasswordLogon	Allow Non Password Logon 0 - No, 1 - Yes, Null - N/A	
AllowNonPasswordLogon_Desc	The display value of AllowNonPasswordLogon (No, Yes, N/A)	
AllowConsoleLogon	Allow Console Logon 0 - No, 1 - Yes, Null - N/A	
AllowConsoleLogon_Desc	The display value of AllowConsoleLogon (No, Yes, N/A)	
AllowRemoteLogon	Allow Remote Logon 0 - No, 1 - Yes, Null - N/A	
AllowRemoteLogon_Desc	The display value of AllowRemoteLogon (No, Yes, N/A)	
HasVisibleRight	Has Visible Right 0 - No, 1 - Yes, Null - N/A	
HasVisibleRight_Desc	The display value of HasVisibleRight (No, Yes, N/A)	
IgnoreDisabled	If this user has 'ignore disabled' right on this computer 0 - No, 1 - Yes, Null - N/A	
IgnoreDisabled_Desc	The display value of IgnoreDisabled (No, Yes, N/A)	

EffectiveUserPrivileges_Computer View

The EffectiveUserPrivileges_Computer view lists consolidated role assignments, logon privileges, and system rights' privileges for each user and computer.

Column Name	Description	Refers to
ADComputer_CanonicalName	The canonical name of the computer	
ADComputer_CnName	The Active Directory computer's common name.	
ADComputer_DnsHostName	The DNS host name of the computer	
ADComputer_ObjectName	The object name of the computer, in the format of <computer CN>.<computer domain>.	

ADUser_CanonicalName	The canonical name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_FullName	The full name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_GUID	The GUID of the assigned Active Directory user. It will be null when trustee type = 7	ADUsers.ADUser_GUID
ADUser_Name	The name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_ObjectName	The display name for the Active Directory user, formatted as <user samAccountName>@<domain name>.	
ADUser_SamAccountName	The samAccount name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_Upn	The upn name of the assigned Active Directory user. It will be null when trustee type = 7	
Assigned_Location	The name of the source assignment location. It might be the zone name, computer dns host name or Computer Role name, depends on the location type	
Assigned_LocationType	The type of the source assignment location 1 – Zone 2 – Computer 3 – Computer Role	
Assigned_LocationTypeDesc	The display value of the source assignment location Zone Computer Computer Role	

Effective_AllowConsoleLogon	If this user has ‘console logon’ right on this computer 0 – No, 1 – Yes, Null – N/A	
Effective_AllowLogon	If this user can logon this computer	
Effective_ AllowNonPasswordLogon	If this user has ‘non password logon’ right on this computer 0 – No, 1 – Yes, Null – N/A	
Effective_ AllowNonRestrictedShell	If this user has ‘non restricted Shell’ right on this computer 0 – No, 1 – Yes, Null – N/A	
Effective_ AllowPasswordLogon	If this user has ‘password logon’ right on this computer 0 – No, 1 – Yes, Null – N/A	
Effective_ AllowPsRemoteAccess	If this user has the 'PowerShell Remote Access' right on this computer 0 - No; 1 - Yes; Null - N/A	
Effective_AllowRemoteLogon	If this user has ‘remote logon’ right on this computer 0 – No, 1 – Yes, Null – N/A	
Effective_AuditLevel	The human readable text of the effective audit level for this user on this computer 0 – Audit not required, 1 –Audit if possible, 2 – Audit required	
Effective_ CloudAuthorizationRequired	If this user has ‘Cloud authorization required’ right on this computer 0 – No, 1 – Yes, Null – N/A	
Effective_HasRescueRight	If this role grants ‘rescue’ right to this user on this computer 0 – No, 1 – Yes	
Effective_HasVisibleRight	Specifies if the user is visible on this computer	
Effective_IgnoreDisabled	If this user has ‘ignore disabled’ right on this computer 0 – No, 1 – Yes, Null – N/A	

EffectiveZone_Id	The ID of the effective zone for the privilege assignment	Zones.Zone_Id Zones_ Hierarchical.Zone_Id
EffectiveZone_Name	The name of the effective zone for the privilege assignment	
Grants_AuditLevel	If this role grants the effective Audit level 0 – Audit not required, 1 – Audit if possible, 2 – Audit required Given the Effective AuditLevel is 0 If this roles's AuditLevel equals to the Effective Audit Level, then this column is 1 – Yes, Otherwise, 0 -- No	
Grants_ CloudAuthorizationRequired	If this role grants 'Cloud authorization required' right to this user on this computer 0 – No, 1 – Yes, Null – N/A	
Grants_ConsoleLogon	If this role grants 'console logon' right to this user on this computer 0 – No, 1 – Yes, Null – N/A	
Grants_HasVisibleRight	Specifies if the role grants the visible right to this user on this computer.	
Grants_IgnoreDisabled	If this role grants 'ignore disabled' right to this user on this computer 0 – No, 1 – Yes, Null – N/A	
Grants_Logon	If this role grants logon	
Grants_NonPasswordLogon	If this role grants 'non password logon' right to this user on this computer 0 – No, 1 – Yes, Null – N/A	
Grants_NonRestrictedShell	If this role grants 'non restricted Shell' right to this user on this computer 0 – No, 1 – Yes, Null – N/A	
Grants_PasswordLogon	If this role grants 'password logon' right to this user on this computer 0 – No, 1 – Yes, Null – N/A	

Grants_PsRemoteAcccess	If this role grants the 'PowerShell Remote Access' right to this user on this computer 0 - No; 1 - Yes; Null - N/A	
Grants_RemoteLogon	If this role grants ‘remote logon’ right to this user on this computer 0 – No, 1 – Yes, Null – N/A	
Grants_RescueRight	If this user has ‘rescue’ right on this computer 0 – No, 1 – Yes	
Right_FullName	The full name of the right. Format in <Right name> / <Right’s zone name>	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	Whether the right applies to windows, unix or both.	
Right_Platform_Desc	The display value of the right platform	
Right_Type	The ID of the right type	RightType.RightTypeId
Right_Type_Desc	The display value of the right type (see RightTypes view)	
Role_FullName	The full name of the role. Format in <Role name> / <Role’s zone name>	
Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	
RoleAssignment_GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_GUID
Trustee_Id	The GUID of the trustee	Trustee_Type = 1: ADUsers.ADUser_GUID Trustee_Type = 2: ADGroups.ADGroup_GUID
Trustee_Name	The name of the trustee	

Trustee_Type	The type of the trustee 1 – Active Directory users 2 – Active Directory groups 7 – All Active Directory users	
Trustee_Type_Desc	The display value of the trustee Active Directory users Active Directory groups All Active Directory users	
ZoneComputer_Id	The zone computer ID	ZoneComputer.ZoneComputer_Id

EffectiveUserPrivileges_ComputerRole_UNIX View

The EffectiveUserPrivileges_ComputerRole_UNIX view lists effective computer role level role assignments for each user. This view assumes that all computers within the computer role are UNIX computers. The assigned Active Directory users must have at least one completed profile in the zone where the computer role is defined. Assignee “All Active Directory users” will be expanded to Active Directory users.

Column Name	Description	Refers to
ADUser_ CanonicalName	The canonical name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_FullName	The full name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_GUID	The GUID of the assigned Active Directory user. It will be null when trustee type = 7	ADUsers.ADUser_GUID
ADUser_Name	The name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_ ObjectName	The general display value for the Active Directory use in the default report. The format is <Active Directory samAccountName>@<domain name>.	
ADUser_ SamAccountName	The samAccount name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_Upn	The upn name of the assigned Active Directory user. It will be null when trustee type = 7	

Assigned_Location	The name of the source assignment location. For this view, it will be always the Computer Role name	
Assigned_ LocationType	The type of the source assignment location 3 - Computer Role	
Assigned_ LocationTypeDesc	The display value of the source assignment location Computer Role	
EffectiveZone_Id	The ID of the effective zone for the privilege assignment	Zones.Zone_Id Zones_ Hierarchical.Zone_Id
EffectiveZone_Name	The name of the effective zone for the privilege assignment	
Right_FullName	The full name of the right. Format in <Right name> / <Right's zone name>	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	The ID of the right platform	
Right_Platform_ Desc	The display value of the right platform	
Right_Type	The ID of the right type	RightType.RightTypeId
Right_Type_Desc	Whether this right is for Unix, Windows or both	
Role_FullName	The full name of the role. Format in <Role name> / <Role's zone name>	
Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
RoleAssignment_ EndTime	The end date and time for the role assignment.	

RoleAssignment_ StartTime	The start date and time for the role assignment.	
Trustee_Id	The GUID of the trustee	If Trustee_Type = 1: ADUsers.ADUser_GUID If Trustee_ Type = 2: ADGroups.ADGroup_GUID
Trustee_Name	The name of the trustee	
Trustee_Type	The type of the trustee 1 – Active Directory users 2 – Active Directory groups 7 – All Active Directory users	TrusteeTypes.TrusteeType_Id
Trustee_Type_Desc	The display value of the trustee Active Directory users Active Directory groups All Active Directory users	

Assigned_LocationType and Assigned_LocationTypeDesc might be removed in subsequent release.

EffectiveUserPrivileges_ComputerRole_Windows View

The EffectiveUserPrivileges_ComputerRole_Windows view lists effective computer role level role assignments for each user. This view assumes that all computers within the computer role are Windows computers. Assignee “All Active Directory users” are NOT expanded to Active Directory users.

Column Name	Description	Refers to
ADUser_ CanonicalName	The canonical name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_FullName	The full name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_GUID	The GUID of the assigned Active Directory user. It will be null when trustee type = 7	ADUsers.ADUser_GUID
ADUser_Name	The name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_ ObjectName	The general display value for the Active Directory use in the default report. The format is <Active Directory samAccountName>@<domain name>.	

ADUser_ SamAccountName	The samAccount name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_Upn	The upn name of the assigned Active Directory user. It will be null when trustee type = 7	
Assigned_Location	The name of the source assignment location. For this view, it will be always the Computer Role name	
Assigned_ LocationType	The type of the source assignment location 3 - Computer Role	
Assigned_ LocationTypeDesc	The display value of the source assignment location Computer Role	
EffectiveZone_Id	The ID of the effective zone for the privilege assignment	Zones.Zone_Id Zones_ Hierarchical.Zone_Id
EffectiveZone_Name	The name of the effective zone for the privilege assignment	
Right_FullName	The full name of the right. Format in <Right name> / <Right's zone name>	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	The ID of the right platform	
Right_Platform_ Desc	The display value of the right platform	
Right_Type	The ID of the right type	RightType.RightTypeId
Right_Type_Desc	Whether this right is for Unix, Windows or both	
Role_FullName	The full name of the role. Format in <Role name> / <Role's zone name>	
Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	

RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
Trustee_Id	The GUID of the trustee	If Trustee_Type = 1: ADUsers.ADUser_GUID If Trustee_ Type = 2: ADGroups.ADGroup_GUID
Trustee_Name	The name of the trustee	
Trustee_Type	The type of the trustee 1 – Active Directory users 2 – Active Directory groups 7 – All Active Directory users	TrusteeTypes.TrusteeType_Id
Trustee_Type_Desc	The display value of the trustee Active Directory users Active Directory groups All Active Directory users	

EffectiveUserPrivileges_Zone_UNIX View

The EffectiveUserPrivileges_Zone view lists effective zone level role assignments for each user. This view assumes that all computers in the zone are UNIX computers. The assigned Active Directory users must have at least one completed profile in the zone. Assignee “All Active Directory users” is expanded to Active Directory users.

Column Name	Description	Refers to
ADUser_ CanonicalName	The canonical name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_FullName	The full name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_GUID	The GUID of the assigned Active Directory user. It will be null when trustee type = 7	ADUsers.ADUser_GUID
ADUser_Name	The name of the assigned Active Directory user. It will be null when trustee type = 7	

ADUser_ ObjectName	The display value for the Active Directory in the default report. The format is <Active Directory samAccountName>@<domain name>.	
ADUser_ SamAccountName	The samAccount name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_Upn	The upn name of the assigned Active Directory user. It will be null when trustee type = 7	
Assigned_Location	The name of the the source assignment location. For this view, it will be always the same as the EffectiveZone_Name	
Assigned_ LocationType	The type of the source assignment location 1 - Zone	
Assigned_ LocationTypeDesc	The display value of the source assignment location Zone	
EffectiveZone_Id	The ID of the effective zone for the privilege assignment	Zones.Zone_Id
EffectiveZone_Name	The name of the effective zone for the privilege assignment	
Right_FullName	The full name of the right. Format in <Right name> / <Right's zone name>	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	Whether this right is for Unix, Windows or both	
Right_Platform_ Desc	The display value of the right platform	
Right_Type	The ID of the right type	RightType.RightTypeId
Right_Type_Desc	The display value of the right type	
Role_FullName	The full name of the role. Format in <Role name> / <Role's zone name>	

Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
Trustee_Id	The GUID of the trustee	if Trustee_Type = 1: ADUsers.ADUser_GUID If Trustee_ Type = 2: ADGroups.ADGroup_GUID
Trustee_Name	The name of the trustee	
Trustee_Type	The type of the trustee 1 - Active Directory users 2 - Active Directory groups 7 - All Active Directory users	TrusteeTypes.TrusteeType_Id
Trustee_Type_Desc	The display value of the trustee: Active Directory users Active Directory groups All Active Directory users	

Assigned_LocationType and Assigned_LocationTypeDesc may be removed in a subsequent release.

EffectiveUserPrivileges_Zone_Windows View

This view lists the effective role assignments for each user, assuming that all computers within the zone are Windows computers. Assignee “All Active Directory users” is NOT expanded to Active Directory users.

Column Name	Description	Refers to
ADUser_ CanonicalName	The canonical name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_FullName	The full name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_GUID	The GUID of the assigned Active Directory user. It will be null when the trustee type = 7	ADUsers.ADUser_GUID

ADUser_Name	The name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_ ObjectName	The display value for the Active Directory in the default report. The format is <Active Directory samAccountName>@<domain name>.	
ADUser_ SamAccountName	The samAccount name of the assigned Active Directory user. It will be null when trustee type = 7	
ADUser_Upn	The UPN name of the assigned Active Directory user. It will be null when trustee type = 7	
Assigned_Location	The name of the the source assignment location. For this view, it will be always the same as the EffectiveZone_Name	
Assigned_ LocationType	The type of the source assignment location 1 - Zone	
Assigned_ LocationTypeDesc	The display value of the source assignment location Zone	
EffectiveZone_Id	The ID of the effective zone for the privilege assignment	Zones.Zone_Id
EffectiveZone_Name	The name of the effective zone for the privilege assignment	
Right_FullName	The full name of the right. Format in <Right name> / <Right's zone name>	
Right_GUID	The GUID of the right	Rights.Right_GUID
Right_Name	The name of the right	
Right_Platform	Whether this right is for Unix, Windows or both	
Right_Platform_ Desc	The display value of the right platform	
Right_Type	The ID of the right type	RightType.RightTypeId
Right_Type_Desc	The display value of the right type	

Role_FullName	The full name of the role. Format in <Role name> / <Role's zone name>	
Role_GUID	The GUID of the role	Roles.Role_Id
Role_Name	The name of the role	
RoleAssignment_ GUID	The object GUID of the role assignment	RoleAssignments.RoleAssignment_ GUID
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
Trustee_Id	The GUID of the trustee	if Trustee_Type = 1: ADUsers.ADUser_GUID If Trustee_ Type = 2: ADGroups.ADGroup_GUID
Trustee_Name	The name of the trustee	
Trustee_Type	The type of the trustee 1 – Active Directory users 2 – Active Directory groups 7 – All Active Directory users	TrusteeTypes.TrusteeType_Id
Trustee_Type_Desc	The display value of the trustee: Active Directory users Active Directory groups All Active Directory users	

EffectiveZoneGroups View

The EffectiveZoneGroups view lists effective group profiles for each computer and zone.

Column Name	Description	Refers to
ZoneGroup_ADGroupGUID	The object GUID of the Active Directory group which the group profile referring to.	ADGroups.GUID
ZoneGroup_ AssignmentLocation_GUID	The object GUID of the assignment location	
ZoneGroup_ AssignmentLocation_Name	The name of the assignment location	

ZoneGroup_ AssignmentLocation_Type	The type code of the assignment location type 1 – Zone, 2 – Computer	
ZoneGroup_ AssignmentLocation_ TypeDesc	(zone/Computer)	
ZoneGroup_Gid	The GID of the group profile	
ZoneGroup_Id	The auto generated ID of the group profile	ZoneGroups.ZoneGroup_Id
ZoneGroup_Name	The UNIX name of the group	
ZoneGroup_ ZoneComputerId	The ID of the computer where the group profile is effective	ZoneComputers.ZoneComputer_Id
ZoneGroup_ZoneId	The ID of the zone where the group profile is defined	Zones.Zone_Id

EffectiveZoneLocalGroupMembers View

This view lists the effective local group members for each computer and zone.

Column Name	Description	Refers to
ZoneLocalGroup_ZoneId	The ID of the zone where the local group profile under	Zones.Zone_Id
ZoneLocalGroup_ ZoneComputerId	The ID of the computer profile where the local group profile effective in	ZoneComputers.ZoneComputer_Id
ZoneLocalGroup_Name	The UNIX name of the local group	
ZoneLocalGroup_ MemberName	The name of the local group's member	
ZoneLocalGroup_ AssignmentLocation_Type	The type code of the assignment location type 1 – Zone, 2 – Computer	
ZoneLocalGroup_ AssignmentLocation_ TypeDesc	(zone/Computer)	
ZoneLocalGroup_ AssignmentLocation_GUID	The object GUID of the assignment location	
ZoneLocalGroup_ AssignmentLocation_Name	The name of the assignment location	

EffectiveZoneLocalGroups View

This view lists the effective local group profiles for each computer and zone.

Column Name	Description	Refers to
ZoneLocalGroup_Id	The auto generated ID of the local group profile	ZoneLocalGroups.ZoneLocalGroup_Id
ZoneLocalGroup_ZoneId	The ID of the zone where the local group profile under	Zones.Zone_Id
ZoneLocalGroup_ ZoneComputerId	The ID of the computer profile where the local group profile effective in	ZoneComputers.ZoneComputer_Id
ZoneLocalGroup_Name	The UNIX name of the group	
ZoneLocalGroup_Gid	The GID of the local group profile	
ZoneLocalGroup_ ProfileState	The profile state of the local group profile 1 = Enabled, 3 = Removed from /etc/group	
ZoneLocalGroup_ ProfileState_Desc	The display value for ZoneLocalGroup_ ProfileState (Enabled/Removed from /etc/group)	
ZoneLocalGroup_ IsCompleteProfile	To indicate if this profile was a complete profile 1 – Yes, 0 - No	
ZoneLocalGroup_ IsCompleteProfile_Desc	The description to the ZoneLocalGroup_IsCompleteProfile (Yes/No)	
ZoneLocalGroup_ AssignmentLocation_Type	The type code of the assignment location type 1 – Zone, 2 – Computer	
ZoneLocalGroup_ AssignmentLocation_ TypeDesc	(zone/Computer)	
ZoneLocalGroup_ AssignmentLocation_GUID	The object GUID of the assignment location	
ZoneLocalGroup_ AssignmentLocation_ Name	The name of the assignment location	

EffectiveZoneLocalUsers View

This view lists the effective local user profiles for each computer and zone.

Column Name	Description	Refers to
ZoneLocalUser_Id	The auto generated ID of the local user profile	ZoneLocalUsers.ZoneLocalUser_Id
ZoneLocalUser_ZoneId	The ID of the zone where the local user profile under	Zones.Zone_Id
ZoneLocalUser_ ComputerProfileId	The name of the zone where the local user profile under	ZoneComputers.ZoneComputer_Id
ZoneLocalUser_ HomeDirectory	The local user profile's home directory	
ZoneLocalUser_Name	The local user profile's unix name	
ZoneLocalUser_ PrimaryGroupId	The local user profile's primary group id	
ZoneLocalUser_ PrimaryGroupName	The local user profile's primary group name	
ZoneLocalUser_GECOS	The local user profile's GECOS	
ZoneLocalUser_Shell	The local user profile's shell	
ZoneLocalUser_Uid	The local user profile's UID	
ZoneLocalUser_ ProfileState	The profile state of the local user 1= Enabled, 2 = Disabled, 3 = Removed from /etc/passwd	
ZoneLocalUser_ ProfileState_Desc	The display value for ZoneLocalUser_ ProfileState (Enabled/Disabled/Removed from /etc/passwd)	
ZoneLocalUser_ IsCompleteProfile	To indicate if this profile was a complete profile 1 - Yes, 0 - No	
ZoneLocalUser_ IsCompleteProfile_Desc	The description to the ZoneLocalUser_ IsCompleteProfile (Yes/No)	

ZoneLocalUser_ AssignmentLocation_ Type	The type code of the location where the zoned user is assigned	
ZoneLocalUser_ AssignmentLocation_ TypeDesc	The display text of the type of the location where the zoned local user is assigned	
ZoneLocalUser_ AssignmentLocation_ GUID	The GUID of the location object where the zoned local user is assigned	
ZoneLocalUser_ AssignmentLocation_ Name	The name of the location object where the zoned local user is assigned	

EffectiveZoneLocalWinGroupMembers View

This view lists the effective local Windows group members for each computer and zone.

Column Name	Description	Refers to
ZoneLocalGroup_ZoneId	The ID for the zone that contains the local Windows group profile	Zones.Zone_Id
ZoneLocalGroup_ ZoneComputerId	The ID of the computer profile where the local Windows group profile is effective	ZoneComputers.ZoneComputer_Id
ZoneLocalGroup_Name	The name of the local Windows group	
ZoneLocalGroup_ MemberName	The name of the local Windows group's member	
ZoneLocalGroup_ AssignmentLocation_Type	The type code of the assignment location type 1 - Zone, 2 - Computer	
ZoneLocalGroup_ AssignmentLocation_ TypeDesc	The display value for ZoneLocalGroup_ AssignmentLocation_Type (zone/Computer)	
ZoneLocalGroup_ AssignmentLocation_GUID	The object GUID of the assignment location	
ZoneLocalGroup_ AssignmentLocation_Name	The name of the assignment location	

EffectiveZoneLocalWinGroups Views

This view lists the effective local Windows group profiles for each computer and zone.

Column Name	Description	Refers to
ZoneLocalGroup_Id	The auto-generated ID of the local Windows group profile	ZoneLocalGroups.ZoneLocalGroup_Id
ZoneLocalGroup_ZoneId	The ID of the zone that contains the local Windows group profile	Zones.Zone_Id
ZoneLocalGroup_ ZoneComputerId	The ID of the computer profile where the local Windows group profile is effective	ZoneComputers.ZoneComputer_Id
ZoneLocalGroup_Name	The name of the local Windows group	
ZoneLocalGroup_ Description	The description of the local Windows group	
ZoneLocalGroup_ ProfileState	The profile state of the local Windows group profile 1 = Enabled, 3 = Removed	
ZoneLocalGroup_ ProfileState_Desc	The display value for ZoneLocalGroup_ ProfileState (Enabled/Removed)	
ZoneLocalGroup_ AssignmentLocation_Type	The type code of the assignment location type 1 - Zone, 2 - Computer	
ZoneLocalGroup_ AssignmentLocation_ TypeDesc	The display value for ZoneLocalGroup_ AssignmentLocation_Type (zone/Computer)	
ZoneLocalGroup_ AssignmentLocation_GUID	The object GUID of the assignment location	
ZoneLocalGroup_ AssignmentLocation_Name	The name of the assignment location	

EffectiveZoneLocalWinUsers View

This view lists the effective local Windows user profiles for each computer and zone.

Column Name	Description	Refers to

ZoneLocalUser_Id	The auto-generated ID of the local windows user profile	ZoneLocalUsers.ZoneLocalGroup_Id
ZoneLocalUser_ZoneId	The ID of the zone that contains the local Windows user profile	Zones.Zone_Id
ZoneLocalUser_ ComputerProfileId	The ID of the computer profile where the local Windows user profile is effective	ZoneComputers.ZoneComputer_Id
ZoneLocalUser_Name	The name of the local Windows user	
ZoneLocalUser_FullName	The full name of the local Windows user	
ZoneLocalUser_ PasswordOption	The password option of the local Windows user	
ZoneLocalUser_ Description	The description of the local Windows user	
ZoneLocalUser_ ProfileState	The profile state of the local Windows user profile 1 = Enabled, 2 = Disabled, 3 = Removed	
ZoneLocalUser_ ProfileState_Desc	The display value for ZoneLocalUser_ ProfileState (Enabled/Disabled/Removed)	
ZoneLocalUser_ AssignmentLocation_ Type	The type code of the assignment location type 1 – Zone, 2 – Computer	
ZoneLocalUser_ AssignmentLocation_ TypeDesc	The display value for ZoneLocalUser_ AssignmentLocation_Type (zone/Computer)	
ZoneLocalUser_ AssignmentLocation_ GUID	The object GUID of the assignment location	
ZoneLocalUser_ AssignmentLocation_ Name	The name of the assignment location	

EffectiveZoneUsers View

The EffectiveZoneUsers view lists effective user profiles for each computer and zone,

Column Name	Description	Refers to
ZoneUser_ ADUserGUID	The object GUID of the Active Directory user which the user profile referring to.	ADUsers.ADUser_GUID
ZoneUser_ AssignmentLocation_ GUID	The GUID of the location object where the zoned user is assigned	
ZoneUser_ AssignmentLocation_ Name	The name of the location object where the zoned user is assigned	
ZoneUser_ AssignmentLocation_ Type	The type code of the location where the zoned user is assigned	
ZoneUser_ AssignmentLocation_ TypeDesc	The display text of the type of the location where the zoned user is assigned	
ZoneUser_ ComputerProfileId	The name of the zone computer where the user profile is effective	ZoneComputers.ZoneComputer_Id
ZoneUser_GECOS	The user profile's GECOS	
ZoneUser_ HomeDirectory	The user profile's home directory	
ZoneUser_Id	The auto generated ID of the user profile	ZoneUsers.ZoneUser_Id
ZoneUser_ IsCompleteProfile	To indicate if this profile was a complete profile 1 - Yes, 0 - No	
ZoneUser_ IsCompleteProfile_ Desc	The description string for ZoneUser_ IsCompleteProfile (Yes/No)	
ZoneUser_IsEnabled	To indicate if this profile was enabled. Only available to classic zone's profile. For hierarchical zone profile, it will always be null 1 - Yes, 0 - No	
ZoneUser_IsEnabled_ Desc	The description string for ZoneUser_ IsEnabled (Yes/No)	

ZoneUser_IsOrphan	1 – It is an orphan user profile. 0 – It is not an orphan profile 1 – Yes, 0 - No	
ZoneUser_IsOrphan_ Desc	The description to the ZoneUser_ IsOrphan (Yes/No)	
ZoneUser_ IsSecondaryProfile	To indicate if this profile was a secondary profile 1 – Yes, 0 - No	
ZoneUser_ IsSecondaryProfile_ Desc	The description string for ZoneUser_ IsSecondaryProfile (Yes/No)	
ZoneUser_Name	The user profile's unix name	
ZoneUser_ PrimaryGroupId	The user profile's primary group id	
ZoneUser_ PrimaryGroupName	The user profile's primary group name	
ZoneUser_Shell	The user profile's shell	
ZoneUser_Uid	The user profile's uid	
ZoneUser_ZoneId	The ID of the zone where the user profile under	Zones.Zone_Id

Rights View

The Rights view lists all rights and system rights defined for each zone.

Column Name	Description	Refers to
Grants_ Logon	Specifies whether the right allows a user to log on to a computer.	
Right_- Description	The description of the right	
Right_-Full-Name	The full name of the right. The format of the full name is: Right_-Name/Right_ZoneName	
Right_-GUID	The object GUID of the right	

Right_-Type	The ID of the right type 1 – Network Access right 2 – Desktop right 3 – Application right 4 – PAM Access right 5 – SSH right 6 – Command right 7 – Restricted Environment 101 – Allow password logon 102 – Allow non password logon 103 – Ignore disabled 104 – Allow non restricted shell 105 – Allow console logon 106 – Allow remote logon 107 – Always permit logon 108 – Audit level – Not required 109 – Audit level – If possible 110 – Audit level – Required 111 – Cloud Authorization Required	RightType.RightTypeId
Right_Type_ Desc	The display value of the right type: Network Access right Desktop right Application right PAM Access right SSH right Command right Restricted Environment Allow password logon Allow non password logon Ignore disabled Allow non restricted shell Allow console logon Allow remote logon Always permit logon Audit level – Not required Audit level – If possible Audit level – Required Cloud Authorization Required	
Right_ZoneId	The zone ID of the right. It will be null for system rights	Zones.Zone_Id
Right_- ZoneName	The zone name of the right. It will be null for system rights	

Rights columns used in other views

Column name	Referred from other view
Rights.Right_ GUID	EffectiveUserPrivileges_Computer.Right_GUID EffectiveUserPrivileges_ ComputerRole.Right_GUID EffectiveUserPrivileges_Zone.Right_GUID

RightType View

The RightType view provides the type of rights that are defined in the zone and what operating system platform the type applies to.

Column Name	Description
Grants_Logon	Specifies if the right can support a user to log on to a system. 0 – No 1 – Yes
RightPlatformId	The platform ID of the right type 0 – Unix 1 – Windows 2 – Unix/Windows
RightTypeDesc	The display value of the right type
RightTypeId	The ID of the right type

RightType columns used in other views

Column name	Referred from other view
RightType.RightTypeId	EffectiveUserPrivileges_Computer.Right_Type EffectiveUserPrivileges_ ComputerRole.Right_Type EffectiveUserPrivileges_Zone.Right_Type Rights.Right_ Type ZoneRolePrivileges.ZoneRolePrivileges_RightType

RoleAssignmentCustomAttribute View

This view lists the role assignment's custom attributes.

Column Name	Description	Refers to
Role_Id	The role's object GUID.	Roles.Role_Id
CustomAttribute_Name	The custom attribute's name.	
CustomAttribute_Value	The custom attribute's value.	

RoleAssignments View

This view lists the role assignments, based on zones, computer roles, or computers.

Column Name	Description	Refers to
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ GUID	The object GUID of the role assignment	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
RoleAssignment_ ZoneId	The ID of the zone where the role assignment belongs to	Zones.Zone_Id
RoleAssignment_ ZoneName	The name of the zone where the role assignment belongs to	
RoleAssignment_ ZoneDomainId	The ID of the domain where the role assignment belongs to	Domains.Id
Assigned_Location	The name of the location where the role assignment is created	
Assigned_ LocationType	The type of the location where the role assignment was created 1 - Zone , 2 - Computer, 3 - Computer Role	

Assigned_ LocationType_Desc	The type description of the location where the role assignment was created 1 - Zone , 2 - Computer, 3 - Computer Role	
RoleAssignment_ TrusteeName	The name of the trustee	
RoleAssignment_ TrusteeType	The type of the trustee 1 - AD user 2 - AD group 3 - Local UNIX user 4 - Local UNIX group 5 - Local Windows user 6 - Local Windows group 7 - All AD users 8 - All UNIX user 9 - All Windows users	
RoleAssignment_ TrusteeType_Desc	The type description of the trustee	
RoleAssignment_ RoleGUID	The object GUID of the assigned role	Roles.Role_Id
RoleAssignment_ RoleName	The name of the assigned role	
RoleAssignment_ RoleFullName	The full name of the assigned role	
RoleAssignment_ Description	The description of the role assignment	

RoleAssignments_Computer View

This view lists the role assignments defined for computers.

Column Name	Description	Refers to
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ GUID	The object GUID of the role assignment	
RoleAssignment_ ZoneComputerId	The ID of the zone computer where the role assignment is defined	ZoneComputers.ZoneComputer_Id
RoleAssignment_ ADComputer_ ObjectName	The name of the zone computer where the role assignment is defined	

RoleAssignment_ ADComputer_ CnName	The Active Directory computer's CN name of the zone computer where the role assignment is defined	
RoleAssignment_ ADComputer_ CanonicalName	The Active Directory computer's canonical name of the zone computer where the role assignment is defined	
RoleAssignment_ ADComputer_ DnsHostName	The Active Directory computer's Dns host name name of the zone computer where the role assignment is defined	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
Computer_Platform	The platform of the zone computer where the role assignment is defined 1 - Windows 2 - UNIX	.
Computer_ Platform_Desc	The platform description of the zone computer where the role assignment is defined 1 - Windows 2 - UNIX	
RoleAssignment_ ZoneId	The ID of the zone where the role assignment belongs	Zones.Zone_Id
RoleAssignment_ ZoneName	The name of the zone where the role assignment belongs	
RoleAssignment_ ZoneDomainId	The ID of the domain where the role assignment belongs	Domains.Id
RoleAssignment_ TrusteeName	The name of the trustee	
RoleAssignment_ TrusteeType	The type of the trustee 1 - AD user 2 - AD group 3 - Local UNIX user 4 - Local UNIX group 5 - Local Windows user 6 - Local Windows group 7 - All AD users 8 - All UNIX user 9 - All Windows users	
RoleAssignment_ TrusteeType_Desc	The type description of the trustee .	
RoleAssignment_ RoleGUID	The object GUID of the assigned role	Roles.Role_Id

RoleAssignment_ RoleName	The name of the assigned role	
RoleAssignment_ RoleFullName	The full name of the assigned role	
RoleAssignment_ Description	The role assignment description	

RoleAssignments_ComputerRole View

The RoleAssignments_Computer Role view lists the role assignments for each computer role.

Column Name	Description	Refers to
RoleAssignment_ ComputerRoleDescription	The description of the Compute Role	
RoleAssignment_ ComputerRoleGUID	The GUID of the Computer Role	
RoleAssignment_ ComputerRoleName	The name of the Computer Role	
RoleAssignment_ Description	The description of the role assignment	
RoleAssignment_EndTime	The end date and time for the role assignment.	
RoleAssignment_GUID	The object GUID of the role assignment	
RoleAssignment_ RoleFullName	The effective end time of the role assignment	
RoleAssignment_RoleGUID	The GUID of the assigned role	Roles.Role_Id
RoleAssignment_ RoleName	The object GUID of the role that is being assigned	
RoleAssignment_StartTime	The start date and time for the role assignment.	
RoleAssignment_ TrusteeName	The trustee name of the role assignment	

RoleAssignment_ TrusteeType	The trustee type code of the role assignment 1 – Active Directory user 2 – Active Directory group 3 – Local UNIX user 4 – Local UNIX group 5 – Local Windows user 6 – Local Windows group 7 – All Active Directory users 8 – All UNIX user 9 – All Windows users	
RoleAssignment_ TrusteeType_Desc	The display value of the trustee type: Active Directory user Active Directory group Local UNIX user Local UNIX group Local Windows user Local Windows group All Active Directory users All UNIX user All Windows users	
RoleAssignment_ ZoneDomainId	The zone's domain ID of the role assignment	Domains.Id
RoleAssignment_ZoneId	The zone ID of the role assignment	Zones.Zone_Id

RoleAssignments_Zone View

This view lists the role assignments defined in zones.

Column Name	Description	Refers to
RoleAssignment_ EndTime	The end date and time for the role assignment.	
RoleAssignment_ GUID	The object GUID of the role assignment	
RoleAssignment_ StartTime	The start date and time for the role assignment.	
RoleAssignment_ ZoneId	The ID of the zone where the role assignment belongs	Zones.Zone_Id
RoleAssignment_ ZoneName	The name of the zone where the role assignment belongs	
RoleAssignment_ ZoneDomainId	The id of the domain where the role assignment belongs	Domains.Id
RoleAssignment_ TrusteeName	The name of the trustee	
RoleAssignment_ TrusteeType	The type of the trustee 1 - AD user 2 - AD group 3 - Local UNIX user 4 - Local UNIX group 5 - Local Windows user 6 - Local Windows group 7 - All AD users 8 - All UNIX user 9 - All Windows users	

RoleAssignment_ TrusteeType_Desc	The type description of the trustee	
RoleAssignment_ RoleGUID	The object GUID of the assigned role	Roles.Role_Id
RoleAssignment_ RoleName	The name of the assigned role	
RoleAssignment_ RoleFullName	The full name of the assigned role	
RoleAssignment_ Description	The description of the role assignment	

RoleCustomAttribute View

This view lists the computer role's custom attributes.

Column Name	Description	Refers to
RoleAssignment_GUID	The role assignment's object GUID.	RoleAssignments.RoleAssignment_GUID
CustomAttribute_Name	The custom attribute's name.	
CustomAttribute_Value	The custom attribute's value.	

RoleRights View

This view lists the rights for each role.

Column Name	Description	Refers to
Role_GUID	The object GUID ID of the role	Roles.Role_Id
Role_-Name	The name of the role	
Role_-Full-Name	The full name of the role. The format of the full name is: <Role_ Name>/<Role_ZoneName>	
Right_GUID	The object GUID of the right	Rights.Right_Id
Right_-Name	The zone name of the right. It will be null for system rights.	

Right_-Full-Name	The full name of the right. The format of the full name is: Right_-Name/Right_ZoneName	
Right_ZoneId	The zone ID of the right. This column is null for system rights.	Zones.Zone_Id
Right_-Type	The ID of the right type 1 – Network Access right 2 – Desktop right 3 – Application right 4 – PAM Access right 5 – SSH right 6 – Command right 7 – Restricted Environment 101 – Allow password logon 102 – Allow non password logon 103 – Ignore disabled 104 – Allow non restricted shell 105 – Allow console logon 106 – Allow remote logon 107 – Always permit logon 108 – Audit level – Not required 109 – Audit level – If possible 110 – Audit level – Required 111 – Cloud Authorization Required	RightType.RightTypeId
Right_Type_ Desc	The display value of the right type: Network Access right Desktop right Application right PAM Access right SSH right Command right Restricted Environment Allow password logon Allow non password logon Ignore disabled Allow non restricted shell Allow console logon Allow remote logon Always permit logon Audit level – Not required Audit level – If possible Audit level – Required Cloud Authorization Required	
Right_-Description	The description of the right	
Right_ Platform	The platform ID of the right 0 – Windows, 1 – UNIX, 2 – Windows/UNIX	
Right_ Platform_ Desc	The platform description of the right (Windows, UNIX, Windows/UNIX)	
Right_ Grants_ Logon	If this right could support a user to logon to a system 1 – Yes, 0 – No	

Roles View

The Roles view lists all roles for each zone. This view is a combined view of the Roles_Classic and Roles_ Hierarchical views.

Column Name	Description	Refers to
Role_-Always-Permit-Logon	(It will be null for classic zone's role) 1 – always permit, 0 – not always permit	

Role_ AlwaysPermitLogon_ Desc	The display value of _-Always-Permit-Logon (It will be null for classic zone's role) (Always permit/Not always permit)	
Role_-Audit-Level	The role's audit level (It will be null for classic zone's role) 0 – audit not required, 1 – audit if possible, 2 – audit required	
Role_AuditLevel_Desc	The display value of Role_AuditLevel (It will be null for classic zone's role) (Audit not Required/Audit if Possible/Audit required)	
Role_-Description	The description of the role	
Role_-Full-Name	The full name of the role. The format of the full name is: <Role_ Name>/<Role_ZoneName>	
Role_-Id	The object GUID of the role	
Role_-Name	The name of the role	
Role_-Zone-Id	The ID of the zone where the role is defined	Zones.Zone_Id
Role_ZoneName	The name of the zone where the role is defined	

Roles Columns Used in Other Views

Column name	Referred from other view
Roles.Right_ GUID	ZoneRolePrivileges.ZoneRolePrivileges_RightGUID
Roles.Role_Id	EffectiveUserPrivileges_Computer.Role_GUID EffectiveUserPrivileges_ComputerRole.Role_ GUID EffectiveUserPrivileges_Zone.Role_GUID RoleAssignments_ ComputerRole.RoleAssignment_RoleGUID ZoneRolePrivileges.ZoneRolePrivileges_ RoleGUID

Roles_Classic View

The Roles_Classic view lists all roles for each classic zone.

Column Name	Description	Refers to
Role_-Always-Permit-Logon	(It will be null for classic zone's role) It is NULL in this view as Audit Level is not applicable in classic zone	

Role_ AlwaysPermitLogon_ Desc	The display value of Role_-Always-Permit-Logon (It will be null for classic zone's role) It is NULL in this view as Audit Level is not applicable in classic zone	
Role_-Audit-Level	The role's audit level (It will be null for classic zone's role) It is NULL in this view as Audit Level is not applicable in classic zone	
Role_AuditLevel_Desc	The display value of Role_AuditLevel (It will be null for classic zone's role) It is NULL in this view as Audit Level is not applicable in classic zone	
Role_-Description	The description of the role	
Role_-Full-Name	The full name of the role. The format of the full name is: <Role_ Name>/<Role_ZoneName>	
Role_-Id	The object GUID of the role	
Role_-Name	The name of the role	
Role_-Zone-Id	The ID of the zone where the role is defined	Zones.Zone_Id
Role_ZoneName	The name of the zone where the role is defined	

Roles_Hierarchical View

The Roles_Hierarchical view lists all roles for each hierarchical zone.

Column Name	Description	Refers to
Role_-Always-Permit-Logon	1 – always permit, 0 – not always permit	
Role_ AlwaysPermitLogon_ Desc	The display value of Role_-Always-Permit-Logon (Always permit/Not always permit)	
Role_-Audit-Level	The role's audit level 0 – audit not required, 1 – audit if possible, 2 – audit required	
Role_AuditLevel_Desc	The display value of Role_AuditLevel (Audit not Required/Audit if Possible/Audit required)	
Role_-Description	The description of the role	

Role_-Full-Name	The full name of the role. The format of the full name is: <Role_ Name>/<Role_ZoneName>	
Role_-ID	The object ID of the role	
Role_-Name	The name of the role	
Role_-Zone-Id	The ID of the zone where the role is defined	Zones.Zone_Id
Role_ZoneName	The name of the zone where the role is defined	

TrusteeTypes View

This view lists the role assignment trustee types.

Column Name	Description	Refers to
TrusteeType_Id	The type ID of the trustee	
TrusteeType_Desc	The type description of the trustee	

Zone_Classic View

The Zones_Classic view lists all Classic zones.

Column Name	Description	Refers to
Zone_AvailableShells	Zone's Available shells	
Zone_CanonicalName	The canonical name of the Zone	
Zone_DefaultGroup	Zone's default group	
Zone_DefaultHomeDirectory	Zone's default home directory	
Zone_DefaultPrimaryGroupId	The default primary group	
Zone_ DefaultPrimaryGroupName	The name of the default primary group	
Zone_DefaultShell	Zone's default shell	
Zone_DomainId	The name of the domain which the Active Directory user belongs to	Domains.Id
Zone_DomainName	The ID of the domain which the Active Directory user belongs to	

Zone_Id	The auto generated ID of the Zone	
Zone_IsHierarchical	If the zone was a Hierarchical zone or not 1 – Is Hierarchical Zone, 0 – Classic Zone	
Zone_IsHierarchical_Desc	The display value for Zone_IsHierarchical (Yes/No)	
Zone_IsSFU	If the zone was a SFU zone or not 1 – SFU Zone, 0 – Non SFU Zone	
Zone_IsSFU_Desc	(Yes/No)	
Zone_Name	The name of the Zone	
Zone_NextGID	Zone's next gid	
Zone_NextUID	Zone's next uid	
Zone_NISDomain	Zone's NIS domain	
Zone_ReservedGID	Zone's reserved gid	
Zone_ReservedUID	Zone's reserved uid	
Zone_SFUDomain	Zone's SFU domain	

Zone_Hierarchical View

The Zones_Hierarchical view lists all Hierarchical zones.

Column Name	Description	Refers to
Zone_AvailableShells	Zone's Available shells	
Zone_CanonicalName	The canonical name of the Zone	
Zone_DefaultGroup	Zone's default group	
Zone_DefaultHomeDirectory	Zone's default home directory	
Zone_DefaultPrimaryGroupId	The default primary group	
Zone_ DefaultPrimaryGroupName	The name of the default primary group	
Zone_DefaultShell	Zone's default shell	

Zone_DomainId	The name of the domain which the Active Directory user belongs to	Domains.Id
Zone_DomainName	The ID of the domain which the Active Directory user belongs to	
Zone_Id	The auto generated ID of the Zone	
Zone_IsHierarchical	If the zone was a Hierarchical zone or not 1 – Is Hierarchical Zone, 0 – Classic Zone	
Zone_IsHierarchical_Desc	The display value for Zone_IsHierarchical 1 – Yes, 0 - No	
Zone_IsSFU	If the zone was a SFU zone or not 1 – SFU Zone, 0 – Non SFU Zone	
Zone_IsSFU_Desc	1 – Yes, 0 - No	
Zone_Name	The name of the Zone	
Zone_NextGID	Zone's next gid	
Zone_NextUID	Zone's next uid	
Zone_NISDomain	Zone's NIS domain	
Zone_ReservedGID	Zone's reserved gid	
Zone_ReservedUID	Zone's reserved uid	
Zone_SFUDomain	Zone's SFU domain	
Zone_ TrustedCloudInstanceUrl	Trusted cloud instance URL	

Zones_Hierarchical Columns Used in Other Views

Column name	Referred from other view
Zones_ Hierarchical.Zone_Id	EffectiveUserPrivileges_Computer.EffectiveZone_Id EffectiveUserPrivileges_ Computer.ZoneUser_Id EffectiveUserPrivileges_ComputerRole.EffectiveZone_Id

ZoneComputers View

The ZoneComputers view lists computer profiles for each zone.

Column Name	Description	Refers to

ZoneComputer_ ADComputerCnName	The Active Directory computer's common name.	
ZoneComputer_ ADComputerDnsHostName	The Active Directory computer's DNS hostname	
ZoneComputer_ ADComputerDomainId	The domain ID of the Active Directory computer which is managed by the zone	
ZoneComputer_ ADComputerId	The object GUID of the Active Directory computer which is managed by the zone	ADComputers.ADComputer_ GUID
ZoneComputer_ ADComputerName	The name of the Active Directory computer which is managed by the zone	
ZoneComputer_ ADComputerObjectName	The object name of the computer, in the format of <computer CN>.<computer domain>.	
ZoneComputer_AgentVersion	The agent version of the managed computer	
ZoneComputer_ ComputerType	The type of the managed computer 1 – Windows, 2 – Unix	
ZoneComputer_ ComputerType_Desc	The display value of the ZoneComputer_ ComputerType (Windows/Unix)	
ZoneComputer_Id	The object GUID of the computer profile	
ZoneComputer_IsHierarchical	1 – It is managed by a hierarchical zone, 0 – It is managed by a classic zone	
ZoneComputer_ IsHierarchical_Desc	The display value of the ZoneComputer_ IsHierarchical (Yes/No)	
ZoneComputer_IsOrphan	1 – It is an orphan profile, 0 – It is not an orphan profile	
ZoneComputer_IsOrphan_ Desc	The display value of the ZoneComputer_ IsOrphan (Yes/No)	
ZoneComputer_IsZoned	If the computer joined zone 1 – Joined zone, 0 – Only has machine overrides	
ZoneComputer_JoinDate	The date when the managed computer joined zone (UTC time)	

ZoneComputer_LicenseType	Specifies the type of computer license. 1 - Server, 2-Workstation, 3-UNIX, 4-Express	
ZoneComputer_ LicenseType_Desc	The description of the license type.	
ZoneComputer_Name	The name of the managed computer	
ZoneComputer_PreferredSite	The preferred site of the computer.	
ZoneComputer_ PreferredSubnetSite	The preferred subnet site of the computer.	
ZoneComputer_ ZoneDomainId	The domain ID of the zone by which the computer is managed	
ZoneComputer_ZoneId	The ID of the zone by which the computer managed	Zones.Zone_Id
ZoneComputer_ZoneName	The name of the zone by which the computer managed	

ZoneComputer Columns Used in Other Views

Column name	Referred from other view
ZoneComputer.ZoneComputer_Id	EffectiveUserPrivileges_Computer.ZoneComputer_Id EffectiveZoneGroups.ZoneGroup_ZoneComputerId EffectiveZoneUsers.ZoneUser_ComputerProfileId

ZoneGroups View

The ZoneGroups view lists group profiles for each zone.

Column Name	Description	Refers to
ZoneGroup_-ADGroup-GUID	The object GUID of the Active Directory group which the group profile referring to.	ADGroups.GUID
ZoneGroup_ ADGroupName	The name of the Active Directory group which the user profile referring to.	
ZoneGroup_-Gid	The group profile's gid	
ZoneGroup_-Id	The auto generated ID of the group profile	

ZoneGroup_ IsOrphan	If the zone group referencing to a valid Active Directory group 1 - It is an orphan user profile. 0 - It is not an orphan profile	
ZoneGroup_ IsOrphan_Desc	The display value for ZoneGroup_IsOrphan 1 - Yes, 0 - No	
ZoneGroup_- Name	The group profile's name	
ZoneGroup_- Zone-Id	The ID of the zone where the group profile is defined	Zones.Zone_Id
ZoneGroup_ ZoneName	The name of the zone where the group profile is defined	

ZoneGroup Columns Used in Other Views

Column name	Referred from other view
ZoneGroups.ZoneGroup_Id	EffectiveUserPrivileges_Computer.ZoneComputer_Id EffectiveZoneGroups.ZoneGroup_ZoneComputerId EffectiveZoneUsers.ZoneUser_ComputerProfileId

ZoneHierarchy View

Column Name	Description	Refers to
ParentZone_Id	The ID of the parent zone.	Zones.Zone_Id
ParentZone_Name	The name of the parent zone.	
ParentZone_DomainID	The domain ID of the parent zone.	Domains.Id
ChildZone_Id	The ID of the child zone.	Zones.Zone_Id
ChildZone_Name	The name of the child zone.	
ChildZone_DomainId	The domain ID of the child zone.	Domains.Id

ZoneLocalGroupMembers View

This view lists the local group members for each zone.

Column Name	Description	Refers to

ZoneLocalGroup_-Id	The auto generated ID of the local group profile	
ZoneLocalGroup_-Zone-Id	The ID of the zone where the local group profile is	Zones.Zone_Id
ZoneLocalGroup_ZoneName	The name of the zone where the local group profile is	
ZoneLocalGroup_-Name	The local group profile's name	
ZoneLocalGroup_MemberName	The name of the local group's member	

ZoneLocalGroups View

This view lists the local group profiles for each zone.

Column Name	Description	Refers to
ZoneLocalGroup_-Id	The auto generated ID of the local group profile	
ZoneLocalGroup_-Zone-Id	The ID of the zone where the local group profile is	Zones.Zone_Id
ZoneLocalGroup_ ZoneName	The name of the zone where the local group profile is	
ZoneLocalGroup_-Gid	The local group profile's GID	
ZoneLocalGroup_-Name	The local group profile's name	
ZoneLocalGroup_ ProfileState	The profile state of the local group profile 1 = Enabled, 3 = Removed from /etc/group	
ZoneLocalGroup_ ProfileState_Desc	The display value for ZoneLocalGroup_ProfileState (Enabled/Removed from /etc/group)	

ZoneLocalUsers View

This view lists the local user profiles for each zone.

Column Name	Description	Refers to
ZoneLocalUser_Id	The auto generated ID of the local user profile	
ZoneLocalUser_ ZoneId	The ID of the zone where the local user profile is	Zones.Zone_Id
ZoneLocalUser_ ZoneName	The name of the zone where the local user profile is	

ZoneLocalUser_ Name	The local user profile's UNIX name	
ZoneLocalUser_ HomeDirectory	The local user profile's home directory	
ZoneLocalUser_ PrimaryGroupID	The local user profile's primary group ID	
ZoneLocalUser_ PrimaryGroupName	The local user profile's primary group name	
ZoneLocalUser_ IsHierarchical	If the zone user was defined in a hierarchical zone or not 1 - It is defined in a hierarchical zone. 0 - Is is defined in a classic zone	
ZoneLocalUser_ IsHierarchical_Desc	The display value for ZoneLocalUser_IsHierarchical (Yes/No)	
ZoneLocalUser_Shell	The shell of the zone user	
ZoneLocalUser_ GECOS	The GECOS of the zone user	
ZoneLocalUser_Uid	The zone user's uid	
ZoneLocalUser_ ProfileFlag	The profile state of the local user 1 means Enabled, 2 means Disabled, 3 means Removed from /etc/passwd	
ZoneLocalUser_ ProfileFlag_Desc	The display value for ZoneLocalUser_ProfileState (Enabled/Disabled/Removed from /etc/passwd)	

ZoneLocalWinGroupMembers View

This view lists the local Windows group members for each zone.

Column Name	Description	Refers to
ZoneLocalGroup_Id	The auto-generated ID of the local Windows group profile	
ZoneLocalGroup_ZoneId	The ID of the zone that contains the local Windows group profile	Zones.Zone_Id
ZoneLocalGroup_ZoneName	The name of the zone that contains the local Windows group profile	
ZoneLocalGroup_Name	The local Windows group profile's name	

ZoneLocalGroup_ MemberName	The name of the local Windows group's member	

ZoneLocalWinGroups View

This view lists the local Windows group profiles for each zone.

Column Name	Description	Refers to
ZoneLocalGroup_Id	The auto-generated ID of the local Windows group profile	
ZoneLocalGroup_ZoneId	The ID of the zone that contains the local Windows group profile	Zones.Zone_Id
ZoneLocalGroup_ZoneName	The name of the zone that contains the local Windows group profile	
ZoneLocalGroup_Name	The local Windows group profile's name	
ZoneLocalGroup_ ProfileState	The profile state of the local Windows group profile 1 = Enabled, 3 = Removed	
ZoneLocalGroup_ ProfileState_Desc	The display value for ZoneLocalGroup_ ProfileState (Enabled/Removed)	

ZoneLocalWinUsers View

This view lists the local Windows user profiles for each zone.

Column Name	Description	Refers to
ZoneLocalUser_Id	The auto generated ID of the local Windows user profile	
ZoneLocalUser_ ZoneId	The ID of the zone where the local Windows user profile is	Zones.Zone_Id
ZoneLocalUser_ ZoneName	The name of the zone where the local Windows user profile is	
ZoneLocalUser_ Name	The local Windows user profile's name	
ZoneLocalUser_ IsHierarchical	If the zone user was defined in a hierarchical zone or not 1 - It is defined in a hierarchical zone. 0 - It is defined in a classic zone	

ZoneLocalUser_ IsHierarchical_Desc	The display value for ZoneLocalUser_IsHierarchical (Yes/No)	
ZoneLocalUser_ FullName	The full name of the local Windows user	
ZoneLocalUser_ Description	The description of the local Windows user	
ZoneLocalGroup_ ProfileFlag	The profile state of the local Windows user profile 1 = Enabled, 2 = Disabled, 3 = Removed	
ZoneLocalGroup_ ProfileFlag_Desc	The display value for ZoneLocalUser_ ProfileState (Enabled/Disabled/Removed)	

ZoneRolePrivileges View

The ZoneRolePrivileges view lists the roles that are defined for each zone and the rights that are granted by each of these roles.

Column Name	Description	Refers to
ZoneRolePrivileges_ RightFullName	The full name of the right	
ZoneRolePrivileges_RightGUID	The GUID of the right	Roles.Right_GUID
ZoneRolePrivileges_RightName	The name of the right	
ZoneRolePrivileges_ RightPlatform	Whether the right is for Unix, Windows or both	
ZoneRolePrivileges_ RightPlatform_Desc	The display value of the right platform	
ZoneRolePrivileges_RightType	The type ID of the right	RightType.RightTypeId
ZoneRolePrivileges_RightType_ Desc	The display value of the right's type	
ZoneRolePrivileges_ RightZoneDomainId	The domain ID of the zone of the right	Domains.Id
ZoneRolePrivileges_RightZoneId	The zone ID of the right	Zones.Zone_Id

ZoneRolePrivileges_ RightZoneIsHierarchical	If the zone of the right is hierarchical 1 - Yes, 0 - No	
ZoneRolePrivileges_ RightZoneIsHierarchical_Desc	The display value of the ZoneRolePrivileges_ RightZoneIsHierarchical (Yes/No)	
ZoneRolePrivileges_ RightZoneName	The zone name of the right	
ZoneRolePrivileges_ RoleFullName	The full name of the role	
ZoneRolePrivileges_RoleGUID	The GUID of the role	Roles.Role_Id
ZoneRolePrivileges_RoleName	The name of the role	
ZoneRolePrivileges_ RoleZoneDomainId	The domain ID of the zone of the domain	
ZoneRolePrivileges_RoleZoneId	The zone ID of the role	Zones.Zone_Id
ZoneRolePrivileges_ RoleZoneIsHierarchical	If the zone of the role is hierarchical 1 - Yes, 0 - No	
ZoneRolePrivileges_ RoleZoneIsHierarchical_Desc	The display value of the ZoneRolePrivileges_ RoleZoneIsHierarchical (Yes/No)	
ZoneRolePrivileges_ RoleZoneName	The zone name of the role	

Zones View

The Zones view lists all the zones in the domain. This view is a combination of both Zones_Classic and Zones_ Hierarchical.

Column Name	Description	Refers to
Zone_AvailableShells	Zone's Available shells	
Zone_CanonicalName	The canonical name of the Zone	
Zone_DefaultGIDType	The ID of the default GID type 1–Use the auto-incremented GID 2–Use the generated GID from the SID 3–Use the Apple GID scheme	

Zone_DefaultGIDType_Desc	The description of the default GID type (Use auto-incremented GID, Generated GID from SID, or Use Apple GID scheme)	
Zone_DefaultGroup	Zone's default group	
Zone_DefaultHomeDirectory	Zone's default home directory	
Zone_DefaultPrimaryGroupId	The default primary group	
Zone_ DefaultPrimaryGroupName	The name of the default primary group	
Zone_DefaultShell	Zone's default shell	
Zone_DefaultUIDType	The ID of the default UID type (applies to hierarchical zones only) 1–Use auto-incremented UID 2–Generated UID from SID 3–Use Apple UID scheme	
Zone_DefaultUIDType_Desc	The description of the default type. For hierarchical zones, this is one of the following: Use auto-incremented UID, Generated UID from SID, or Use Apple UID scheme. For classic zones: Use auto-incremented UID.	
Zone_DefaultUserName	The description of the zone scheme ID, such as Standard, RFC 2307, or SFU.	
Zone_DomainId	The name of the domain which the Active Directory user belongs to	Domains.Id
Zone_DomainName	The ID of the domain which the Active Directory user belongs to	
Zone_Id	The auto generated ID of the Zone	
Zone_IsHierarchical	If the zone was a Hierarchical zone or not 1 - Is Hierarchical Zone, 0 - Classic Zone	
Zone_IsHierarchical_Desc	If the zone was a Hierarchical zone or not (Yes/No)	
Zone_IsSFU	If the zone was a SFU zone or not 1 - SFU Zone, 0 - Non SFU Zone	
Zone_IsSFU_Desc	If the zone was a SFU zone or not (Yes/No)	
Zone_Name	The name of the Zone	
Zone_NextGID	Zone's next gid	

Zone_NextUID	Zone's next uid	
Zone_NISDomain	Zone's NIS domain	
Zone_ReservedGID	Zone's reserved gid	
Zone_ReservedUID	Zone's reserved uid	
Zone_Schema	The ID of the zone scheme: 1–Standard 2–RFC 2307 3–SFU	
Zone_SFUDomain	Zone's SFU domain	
Zone_Type	The zone type (hierarchical or classic)	
Zone_ TrustedCloudInstanceUrl	Trusted cloud instance URL	

Zone view columns used in other views

Column name	Referred from other view
Zone.Zone_Id	Roles_Classic.Role_ZoneId ComputerRoleMembership.ComputerRole_ZoneId ComputerRoleMembership.ZoneComputer_ZoneId EffectiveUserPrivileges_ Computer.EffectiveZone_Id EffectiveUserPrivileges_ComputerRole.EffectiveZone_Id EffectiveUserPrivileges_Zone.EffectiveZone_Id EffectiveZoneGroups.ZoneGroup_ZoneId EffectiveZoneUsers.ZoneUSer_ZoneId Rights.Right_Id RoleAssignments_ ComputerRole.RoleAssignment_ZoneId Roles.Role_ZoneId Roles_Hierarchical.Role_ZoneId ZoneComputers.ZoneComputer_ZoneId ZoneGroups.ZoneGroup_ZoneId ZoneRolePrivileges.ZoneRolePrivileges_RoleZoneId ZoneRolePrivileges.ZoneRolePrivileges_RightZoneId ZoneUsers.ZoneUser_ZoneId

ZoneUsers View

The ZoneUsers view lists the user profiles for each zones.

Column Name	Description	Refers to
ZoneUser_ ADUserGUID	The object GUID of the Active Directory user which the user profile referring to.	ADUsers.ADUser_ GUID
ZoneUser_ ADUserName	The name of the Active Directory user which the user profile referring to.	
ZoneUser_GECOS	The GECOS of the zone user	

ZoneUser_ HomeDirectory	The user profile's home directory	
ZoneUser_Id	The auto generated ID of the user profile	
ZoneUser_ IsHierarchical	If the zone user was defined in a hierarchical zone or not 1 – It is defined in a hierarchical zone. 0 – Is is defined in a classic zone	
ZoneUser_ IsHierarchical_Desc	The display value for ZoneUser_IsHierarchical (Yes/No)	
ZoneUser_IsOrphan	If the zone user referencing to a valid Active Directory user 1 – It is an orphan user profile. 0 – It is not an orphan profile	
ZoneUser_IsOrphan_ Desc	The display value for ZoneUser_IsOrphan (Yes/No)	
ZoneUser_IsSFU	If the zone user was defined in a SFU zone or not 1 – It is defined in a SFU zone. 0 – Is is not defined in a SFU zone	
ZoneUser_IsSFU_ Desc	The display value for ZoneUser_IsSFU (Yes/No)	
ZoneUser_Name	The user profile's unix name	
ZoneUser_ PrimaryGroupID	The user profile's primary group id	
ZoneUser_ PrimaryGroupName	The user profile's primary group name	
ZoneUser_Shell	The shell of the zone user	
ZoneUser_Uid	The zone user's uid	
ZoneUser_ UserEnabled	If the zone user is enabled (For classic zone user only, it will be null for Hierarchical zone user) 1 – enabled, 0 – disabled, NULL – not applicable	
ZoneUser_ UserEnabled_Desc	(Yes/No)	
ZoneUser_ZoneId	The ID of the zone where the user profile under	Zones.Zone_Id
ZoneUser_ZoneName	The name of the zone where the user profile under	

ZoneUser Columns Used in Other Views

Column name	Referred from other view
ZoneUsers.ZoneUser_Id	EffectiveUserPrivileges_Computer.ZoneUser_Id EffectiveUserPrivileges_ ComputerRole.ZoneUser_Id EffectiveUserPrivileges_Zone.ZoneUser_Id EffectiveZoneUsers.ZoneUser_Id

Troubleshooting Reports

In general, if something doesn't work the way that you think it should, try the following to troubleshoot your reporting environment:

- View the log files
- Rebuild or refresh the reporting data
- Validate that the reporting service has the correct permissions to read data from the monitored domains and replicate the data.
- Export diagnostics data for use by Delinea Technical Support (if technical support requests that you do so).

This section describes some situations that you might encounter, along with some suggested solutions or workarounds.

You Don’t See Any data When You Open a Report

Problem: You’ve installed everything and you can open a report, but you don’t see any data.

Solution: Make sure that there has been at least one synchronization between Active Directory and the reporting database. Use the Report Configuration wizard to do this.

You Don’t See the Report Builder Link in Internet Explorer

Problem: You go the Home page in Internet Explorer, the home page for your deployed reports in SSRS, and you do not see the Report Builder link. But you’re fairly sure that you have the required permissions to create reports.

Solution: Here are some things for you to check:

1. Make sure that you are logging in within the same domain that SSRS is installed within. For example, if you’re creating an evaluation version that uses a different domain, there may be issues.
2. Go download the Report Builder for your SQL Server version. For now, it’s a separate download.

You Can’t Log in to Report Services in Internet Explorer

Problem: When you log in to Delinea Report Services in Internet Explorer, you cannot successfully log in. You see an error message like this: “User domain\user does not have required permissions. Verify that sufficient permissions have been granted and Windows User Account Control (UAC) restrictions have been addressed.”

Explanation: If you're seeing this issue, it may have happened after your first installation or an upgrade in which you created a new SQL Server instance.

Solution: Here are some things for you to try:

- When you go to launch Report Services, right-click it and select Run as Administrator. This may allow you to log in to Report Services, and from there you can edit the Site Settings for security.
- Log in to Report Services as an administrator, and go to Site Settings to add your users by way of adding the domain and assign the group or user a role. For details, see Granting access in SSRS to reports.
- Make sure that you also set permissions for the home folder, as mentioned in the topic mentioned above.

You Get a Server Error When You Try to Synchronize with Active Directory

Problem: In the Report Services control panel, when you go to synchronize data for report services, the following error displays: "The server is unwilling to process the request." (KB-6350)

You also see a similar error in the report services log file. Here's an example of what the error looks like:

[2015-08-21 10:53:25.714 +0800] Centrify.Report.Service.exe[3596,10] Error: SyncServer.DoSynchronization: Failure during synchronize domain a9f1r1.test, DC: a9d1-w2k12r2.a9f1r1.test.

[2015-08-21 10:53:25.714 +0800] Centrify.Report.Service.exe[3596,10] Error: SyncServer.DoSynchronization: Reason: The server is unwilling to process the request.

Explanation: The issue is due to insufficient memory on the domain controller. The domain controller is unable to allocate enough memory for Active Directory caching.

Solution: Adjust the memory allocated to the domain controller, according to Memory requirements.

Port Conflicts

Problem: Delinea Report Services not install correctly when port 80 is used by another application, such as Apache Tomcat. The following error displays during the report services configuration wizard: "The service was unable to access Report Services." (KB-7443)

Explanation: By default, Microsoft SQL Server Reporting Services (SSRS) use port 80, and it is not recommended to run it with a third party software that also uses port 80 or 443.

Solution: For port conflict situations, you can configure SSRS to use another port.

To change the port that SQL Server Reporting Services (SSRS) uses:

1. Open the SQL Server Reporting Services Configuration Manager.
2. Navigate to the **Web Service URL**.
3. Change the TCP port to an unused port other than 80.

For example, port 8080.

4. Navigate to the **Report Manager URL**, and click **Advanced**.
5. Change the TCP port to the same port number that you specified in Step 3.
6. Run the Delinea Report Services Configuration Wizard and specify URLs with the new port number.

For example, `http://reportservice:8080/ReportServer_CssREPORTS2`

7. Verify that you can access reports through the specified port.

You may also need to modify your firewall rules for access to the specified port.

SSRS Fails to Start on Windows 2008 R2 Systems

Problem: SQL Server Reporting Services (SSRS) fails to start, due to a timeout issue. This issue occurs only on Windows 2008 R2 systems. (KB-8065)

SSRS Produces the Following Error

Windows could not start the SQL Server Reporting Services (MSSQLSERVER) service on local computer. Error 1053: The service did not respond to the start or control request in a timely fashion.

Explanation: This happens due to SSRS checking for certificate revocation lists (CRL), and this is a Microsoft known issue, as detailed here: http://support.microsoft.com/kb/2745448.

Delinea does not take any responsibility for the content or availability of this link, it is provided as a courtesy. You should contact Microsoft if there are any further questions.

Solution: You can perform one of the following tasks to try and resolve this issue:

- Disable certificate revocation lists checking. For details, see http://tech.lanesnotes.com/2014/02/sql-server-reporting-services-service.html
- Change the default revocation checking behavior using group policy. For details, see https://technet.microsoft.com/en-us/library/ee619786(v=ws.10).aspx

SQL Server 2008 R2 Express Edition Produces an Installation Error

Problem: When you run the installer, you get an error when it tries to install the SQL Server 2008 R2 Express edition for report services. The installer produces the following error: (KB-8172)

The Report Services Configuration Wizard Cannot be Completed Due to an Error that Occurred

The program was unable to install SQL Server on this computer, exit code: 0x851A0017. Please refer to the Delinea Knowledge Base article (KB-4589) for more information on the error code you received. Please fix the issue and run Setup again.

You might also see something like the following errors in the SQL Server log file, which you can locate in a directory such as C:\Program Files\Microsoft SQL Server\100\Setup Bootstrap\Log\<number>\Detail.txt.

2017-01-25 12:41:31 Slp: Configuration action failed for feature SQL_Engine_Core_Inst during timing ConfigRC and scenario ConfigRC. 2017-01-25 12:41:31 Slp: Could not find the Database Engine startup handle. 2017-01-25 12:41:31 Slp: The configuration failure category of current exception is ConfigurationFailure 2017-01-25 12:41:31 Slp: Configuration action failed for feature SQL_Engine_Core_Inst during timing ConfigRC and scenario ConfigRC. 2017-01-25 12:41:31 Slp: Microsoft.SqlServer.Configuration.SqlEngine.SqlEngineConfigException: Could not find the Database Engine startup handle. 2017-01-25 12:41:31 Slp: at Microsoft.SqlServer.Configuration.SqlEngine.SqlServerServiceBase.WaitSqlServerStart(Process processSql)

2017-01-25 12:41:31 Slp: at Microsoft.SqlServer.Configuration.SqlEngine.SqlEngineDBStartConfig.ConfigSQLServerSystemDatabases (EffectiveProperties properties, Boolean isConfiguringTemplateDBs, Boolean useInstallInputs) 2017-01-25 12:41:31 Slp: at Microsoft.SqlServer.Configuration.SqlEngine.SqlEngineDBStartConfig.DoCommonDBStartConfig (ConfigActionTiming timing) 2017-01-25 12:41:31 Slp: at Microsoft.SqlServer.Configuration.SqlConfigBase.SlpConfigAction.ExecuteAction(String actionId) 2017-01-25 12:41:31 Slp: at Microsoft.SqlServer.Configuration.SqlConfigBase.SlpConfigAction.Execute(String actionId, TextWriter errorStream) 2017-01-25 12:41:31 Slp: Exception: Microsoft.SqlServer.Configuration.SqlEngine.SqlEngineConfigException. 2017-01-25 12:41:31 Slp: Source: Microsoft.SqlServer.Configuration.SqlServer_ConfigExtension. 2017-01-25 12:41:31 Slp: Message: Could not find the Database Engine startup handle.

Explanation: The SQL Server Express edition isn't able to use the encryption protocols provided by the server.

The installation error occurs because TLS1.0/1.1 and SSL 3.0 protocols and some ciphers have been disabled on the server, due to customer security concerns. SQL Server 2008 R2 Express Edition does not support the newer version of cipher suites (such as TLS1.2 with SHA256), while the regular versions of SQL Server with the latest updates or support packs (SP) do.

Solution: Restore the server settings back to the system defaults that allow TLS1.0/1.1, SSL 3.0 protocols and ciphers. After you do that, the installer will successfully complete a report services installation with SQL Server Express edition.

Installing SQL Server from the Delinea Management Services Installer Generates Error Codes

Problem: When you install the SQL Server version that is bundled with the Delinea Management Services installer, there are errors. (KB-4589)

SQL Server installation error	Description
0x84B40000 - full text service cannot run under local system account on DC.	This means user is trying to install SQL Server on a Domain Controller with Full Text Search service configured under a local system account. This is not supported by Microsoft. Workaround is to either install SQL on a member server, or manually install SQL and select a different account to run it as Full Text Search service.
	For this error code, more information is needed, see below on how to collect logs.

0X6AA	If SQL server is already installed on a machine with default SQL server instance (with advanced services), the SQL server setup will fail with the above error code. To workaround this issue, reinstall SQL Native Client (SNAC) before installing the second instance of SQL Server 2005 Express Edition with Advanced Services. - http://msdn.microsoft.com/en-us/sqlserver/ff658533 (Provided as a courtesy)
	This means a hyphen (-) in the SQL server's instance name has been specified and is not allowed.
	SQL Server Management Studio 2005 has been installed on the system and there is an attempt to install SQL 2008 on top of it. To workaround this issue, manually uninstall SQL Server Management Studio and then install the later version.
	PowerShell 2.0, which is a prerequisite for Microsoft SQL server 2014, is not installed. Install Windows Management Framework 2.0 first before run Report Services Configuration Wizard
	SQL Server 2008 R2 express edition with advanced features will fail to install an new instance when TLS 1.0/1.1 and SSL 3.0 protocols are disabled. It fails with a message like: SQL Server installation failed. To continue, investigate the reason for the failure, correct the problem, uninstall SQL Server, and then rerun SQL Server Setup. To work around this issue, re-enable the protocols (Update corresponding values to 1.) The SQL Server instance then can be installed successfully. Refer to: https://blogs.msdn.microsoft.com/friis/2016/07/25/disabling-tls-1-0-on-your-windows-2008-r2-server-just-because-you-still-have-one/

If the SQL Server installation fails for any other reason, send the installation log files to Delinea support. You can locate the installation log files in the following locations:

- SQL Server 2008 and 2008 R2:

%ProgramFiles%\Microsoft SQL Server\100\Setup Bootstrap\LOG

- SQL Server 2012:

%ProgramFiles%\Microsoft SQL Server\110\Setup Bootstrap\Log\.

- SQL Server 2014:

%ProgramFiles%\MicrosoftSQL Server\120\Setup Bootstrap\Log\.

- SQL Server 2016:

%ProgramFiles%\ Microsoft SQL Server\130\Setup Bootstrap\Log\

See also: https://centrify.my.salesforce.com/50180000000bIYD, http://support.microsoft.com/kb/955396.

Can’t install SQL Server 2012 or 2014 instance on Windows 2008 SP2

Problem: If you use the Report Services Configuration wizard to install a new instance of SQL Server version 2012 or 2014 on Windows Server 2008 SP2, the installation fails if Windows Powershell 2.0+ or Windows Management Framework 2.0 is not already installed. The installation failure has an exit code of 0x84BE0260 (KB-7096).

Explanation: Windows Server 2008 SP2 doesn't include PowerShell 2.0 or Windows Management Framework 2.0 by default. Later versions of Windows Server do include these components by default.

Solution: Install PowerShell 2.0 or higher and Windows Management Framework 2.0 before you run the Report Services Configuration Wizard to install a new instance of Microsoft SQL Server 2012 or 2014.

You can download Windows Management Framework 2.0 from https://support.microsoft.com/en-us/kb/968930.

Report Services computation takes longer than it used to

Problem: If Report Services uses SQL Server 2014 or above, you might notice that Report Services spends more time on computation.

Explanation: In SQL Server 2014, Microsoft introduced a new cardinality estimator (CE). This cardinality estimator was redesigned to improve query performance, and there may be some performance degradation for some SQL statements.

Solution: If you notice some report services computation performance issues, set the database compatibility level to 110 to force SQL Server to use the old cardinality estimator.

To set the database compatibility level to 110:

1. In SQL Server Management studio, run the following before Report Services synchronizes with Active Directory:

ALTER DATABASE <the database name deployed by Report Services> SET COMPATIBILITY_LEVEL = 110

Frequently asked questions about report services

Question: Is it possible for report services to use an existing database that's already been created according to our organization's standards?

Answer: Report services cannot use an existing database, the Configuration Wizard creates a new database.

Question: Does report services create just one database?

Answer: Yes. If you reconfigure report services, the Configuration Wizard creates a new database.

Question: Does the report services installation make any other modifications to database objects other than in the database it creates?

Answer: No.