Sybase 15 ASE (PC)

Thank you for your interest in authenticated compliance scanning! When you use authentication, you get a more in-depth assessment of your hosts and the most accurate results. This document provides tips and best practices for authenticating to Sybase Adaptive Server Enterprise (ASE) instances.

A few things to consider

Why should I use authentication?

With authentication we can remotely log in to each target system with credentials that you provide, and because we're logged in we can do more thorough testing. This will give you better visibility into each system's security posture. Is it required? Yes, it's required for compliance scans.

Are my credentials safe?

Yes, credentials are exclusively used for READ ACCESS ONLY to your system. The service does not modify or write anything on the device in any way. Credentials are securely handled by the service and are only used for the duration of the scan.

Which technologies are supported?

For the most current list of supported authentication technologies and the versions that have been certified for VM and PC by record type, please refer to the following article:

Authentication Technologies Matrix

What are the steps?

First, set up a Sybase Authentication account and privileges on target hosts (we'll help you with this below). Then, using Qualys Policy Compliance, complete these steps: 1) Add Sybase authentication records. 2) Launch a compliance scan. 3) Run the Authentication Report to view the authentication status (Passed or Failed) for each scanned host.

Sybase Setup

In order for the Qualys Compliance Scan to work properly on a Sybase database, the following account and privileges must exist prior to running the scan. Note – These scripts require a super-user account. For example, sa or an administrator account. (Starting with Sybase 15.7, the way to create logins and users has changed. If you are operating on a Sybase 15.7 or newer installation, please move to step 1b.)

1a) Create a Login for the Scan Account (Sybase versions 15.5 and earlier)

This script creates a database login for the user account to be used for scanning. Please provide a password and the name of the target database before running the script. Tip – We recommend creating an account called QUALYS_SCAN.

USE master

Copyright 2015-2022 by Qualys, Inc. All Rights Reserved.

```
GO
sp_addlogin "QUALYS_SCAN", "[strong password]"
GO
```

1b) Create a Login for the Scan Account (Sybase versions 15.7 and later)

```
USE master
GO
create login QUALYS_SCAN with password  "[strong password]"
GO
```

2) Create a User Account

This script creates a user account, called QUALYS_SCAN, in the target databases, master, sybsystemprocs, sybsecurity (if audit is installed) respectively.

```
USE master
GO
sp_adduser QUALYS_SCAN
GO

USE sybsystemprocs
GO
sp_adduser QUALYS_SCAN
GO

USE sybsecurity
GO
sp_adduser QUALYS_SCAN
GO
```

3) Grant Privileges to the Scan Account

This script grants privileges to the user account to be used for scanning. The following privileges are required for successful authentication and compliance scanning. The sybsecurity database will only exist after auditing installation process is completed.

```
USE master
GO
grant select on master.dbo.syslogins to QUALYS_SCAN
grant select on master.dbo.sysdatabases to QUALYS_SCAN
grant select on master.dbo.sysconfigures to QUALYS_SCAN
grant select on master.dbo.sysprotects to QUALYS_SCAN
grant select on master.dbo.sysattributes to QUALYS_SCAN
grant select on master.dbo.syssrvroles to QUALYS_SCAN
grant select on master.dbo.sysloginroles        to QUALYS_SCAN
grant select on master.dbo.sysusers to QUALYS_SCAN
grant select on master.dbo.sysobjects to QUALYS_SCAN
GO

USE sybsystemprocs
GO
grant select on sybsystemprocs.dbo.sysobjects to QUALYS_SCAN
GO
```

```
USE sybsecurity
GO
grant select on sybsecurity..sysauditoptions to QUALYS_SCAN
GO
```

4) Grant the Scan Account access to sso_role (optional)

For certain controls, being a member of the sso_role will be required. These controls will only access information via stored procedures and will not modify or write to the system. The controls affected by this are Control IDs 8706 and 8728. Please understand, we know that this isn't least privilege, but to obtain the information needed, the scan account needs sso_role.

```
USE master
GO
grant role sso_role to QUALYS_SCAN
GO
```

5) Check Privileges on the Scan Account

We provide a script in the zip archive to help you identify missing privileges from the user account to be used for scanning. This script is in the file QG_Sybase_Auth_verx.x.txt. The script should be executed by a super-user against a database to determine if all the appropriate privileges have been setup correctly. The script will generate an output listing the status of all the prerequisites.

Sample output

Prerequisites	Status
dbo	<---Current logged on user
QUALYS_SCAN	PASSED – account exists
SSO_ROLE	PASSED – member of role
SYSLOGINS	PASSED – SELECT privilege exists
SYSDATABASES	PASSED – SELECT privilege exists
SYSCONFIGURES	PASSED – SELECT privilege exists
SYSPROTECTS	PASSED – SELECT privilege exists
SYSATTRIBUTES	PASSED – SELECT privilege exists
SYSSRVROLES	PASSED – SELECT privilege exists
SYSLOGINROLES	PASSED – SELECT privilege exists
SYSUSERS	PASSED – SELECT privilege exists
SYSOBJECTS	PASSED – SELECT privilege exists
SYBSYSTEMPROCS.SYSOBJECTS	PASSED – SELECT privilege exists
VERSION	16000

Prerequisites	Status
SYSAUDITOPTIONS	PASSED – SELECT privilege exists

Did you get different results? Contact your Sybase DBA to ensure that privileges are set up correctly.

Sybase Authentication Records

You'll need to create a separate authentication record for each Sybase instance to be scanned. Create Sybase records from the Policy Compliance (PC) application.

How do I get started?

Go to Scans > Authentication > New > Databases Sybase.

Tell us the username and password to use for authentication. Then enter the database name you want to authenticate to and the port the database is on. We'll find the Sybase ASE instance based on the port number you enter. Scanning Unix hosts? You'll also need to tell us the database installation directory.

Enter the compliance hosts you want to scan in the IPs section, click Save to save your record, and that's it! You're ready to scan.

Note – The database name and port combination must be unique in each record. To scan multiple database instances, add additional Sybase records.

Sample Sybase Record

Last updated: May 27, 2022