CHAPTER

SQL Password Security

3

INFORMATION IN THIS CHAPTER:

- SQL Server Password Security
- Strong Passwords
- Contained Database Logins in SQL Server 2012
- Encrypting Client Connection Strings
- Application Roles
- Using Windows Domain Policies to Enforce Password Length
- Contained Databases
- Summary

SQL SERVER PASSWORD SECURITY

One of the key ways to protect your SQL Server is to use strong, secure passwords for your SQL Server login accounts. One of the biggest security holes in the SQL Server 2000 and older versions of Microsoft SQL Server was that the server was installed with a blank system administrator (SA) password by default and would allow you to use a blank password, thereby permitting anyone to connect without much work at all.

Even with newer versions of Microsoft SQL Server, the SA account is still a potential weakness, as is any SQL Server Authentication based login. This is because SQL accounts can be easily broken into by brute force password attacks. When using SQL Azure there is no SA account available to you, the Microsoft customer to work with. The SA account is reserved for the exclusive use of Microsoft.

When using SQL Azure as your database instance, only SQL Authentication is available. SQL Azure doesn't support Windows Authentication for use by Microsoft's customers as the SQL Azure database server doesn't support being added to a company domain. The Azure database servers do support Windows Authentication only for use by the Azure administration team within Microsoft.

SQL Authentication Logins are more susceptible to these login attacks than a Windows Authentication Login because of the way that these logins are processed. With an SQL Authentication Login, each connection to the SQL database passes the

Securing SQL Server http://dx.doi.org/10.1016/B978-1-59-749947-7.00003-4