

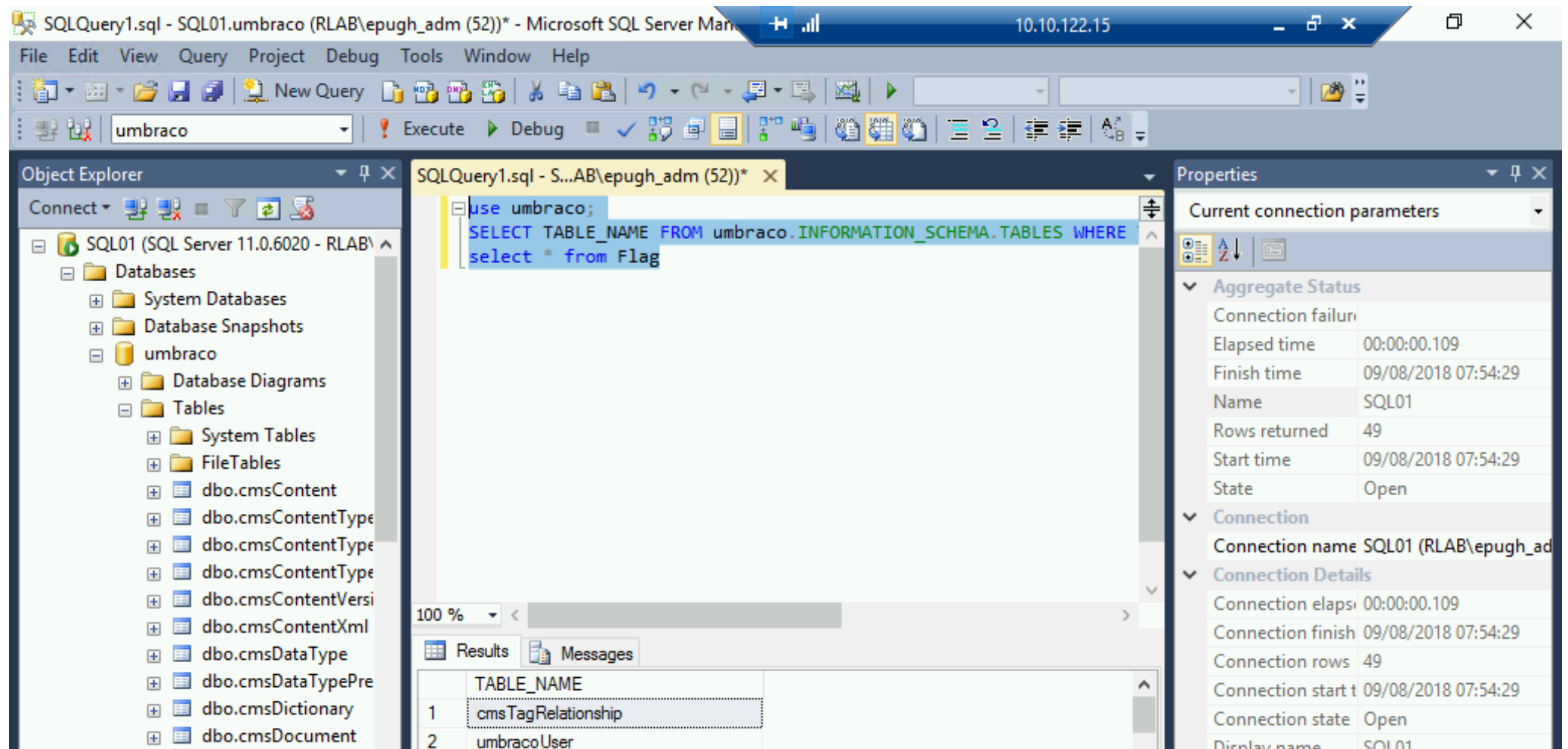
using epugh_adm creds, logged in to web01 (10.10.110.10) and from there took rdp of sql01(10.10.122.15) using same creds.

start sql mangement studio,
connect via windows authentication,

use umbraco;

```
SELECT TABLE_NAME FROM umbraco.INFORMATION_SCHEMA.TABLES WHERE TABLE_TYPE = 'BASE TABLE'
```

```
select * from Flag
```



The screenshot displays the Microsoft SQL Server Enterprise Manager interface. The central pane shows a query window with the following SQL code:

```
use umbraco;  
SELECT TABLE_NAME FROM umbraco.INFORMATION_SCHEMA.TABLES WHERE  
TABLE_TYPE = 'BASE TABLE';  
select * from Flag
```

The left pane (Object Explorer) shows the database structure for 'SQL01 (SQL Server 11.0.6020 - RLAB\epugh_adm)'. The 'Databases' folder is expanded, showing 'System Databases', 'Database Snapshots', 'umbraco', 'Database Diagrams', and 'Tables'. The 'Tables' folder is expanded, showing 'System Tables', 'FileTables', and a list of tables including 'dbo.cmsContent', 'dbo.cmsContentType', 'dbo.cmsContentVersion', 'dbo.cmsContentXml', 'dbo.cmsDataType', 'dbo.cmsDataTypePre', 'dbo.cmsDictionary', and 'dbo.cmsDocument'.

The bottom pane (Results) shows the execution results of the query, displaying two rows:

TABLE_NAME
cms TagRelationship
umbracoUser

The right pane (Properties) shows the 'Current connection parameters' for the connection 'SQL01 (RLAB\epugh_adm)'. The 'Aggregate Status' section shows the connection is open, with a finish time of 09/08/2018 07:54:29 and 49 rows returned. The 'Connection' section shows the connection name 'SQL01 (RLAB\epugh_adm)' and the connection state 'Open'.

The screenshot displays the Microsoft SQL Server Enterprise Manager interface. On the left, a tree view shows the database structure, including tables like 'dbo.cmsDocumentTy', 'dbo.cmsLanguageTe', 'dbo.cmsMacro', 'dbo.cmsMacroPropert', 'dbo.cmsMember', 'dbo.cmsMember2Me', 'dbo.cmsMemberType', 'dbo.cmsPreviewXml', 'dbo.cmsPropertyData', 'dbo.cmsPropertyType', and 'dbo.cmsPropertyType'. The central pane shows a query result for the 'cmsTask' table, with the 'flag' column highlighted. The result is 'RASTA{d474b4535_4r3_u5u4lly_1n73r3571n6}'. The status bar at the bottom indicates 'Query e...' and '49 rows'.

Display name	SQL01
Login name	RLAB\epugh_adm
Server name	SQL01
Server version	11.0.6020
Session Tracing ID	
SPID	52

Name	The name of the connection.

Ready Ln 1 Col 1 Ch 1 INS

08:01 09/08/2018

RASTA{d474b4535_4r3_u5u4lly_1n73r3571n6}