Shavlik Protect

Report Views Guide

Copyright

Trademarks

Document Information and Print History

Document number: N/A

Date	Version	Description
January 2014	Initial release	Initial release of the *Report Views Guide*.
April 2014	Shavlik Protect 9.1	Add DeployState query.
September 2015	Shavlik Protect 9.2	Add Deployid to PatchDeployment view. In Patch view, remove Name and add BulletinTitle.

OVERVIEW

This document describes how to use database views within SQL Server database queries to generate custom reports for Shavlik Protect.

When you install Shavlik Protect it creates a number of defined views in the Protect SQL Server database. You can reference these views within custom queries that you write to extract exactly the information you want. By executing the custom queries and exporting the results to the format of your choice you effectively create your own customized reports for Shavlik Protect.

The benefits of writing your own database queries are:

- You can mine the Protect database for the exact information you want.

  You can go beyond the predefined reports provided within Shavlik Protect. While the predefined reports are sufficient for many organizations, you may have the need to produce one or more custom reports that provide more specific information about the status of your machines.

- You can export the query results and present the information in the format of your choosing.

You can, of course, opt to write custom queries without using the Protect views. When you add the use of Protect views to your custom queries, however, you gain a number of other benefits:

- The view schemas will not change in future versions of Shavlik Protect.

  Future versions of Shavlik Protect may modify the tables in the database. By referencing Protect views in your queries rather than the tables, you will be guaranteed that your custom queries will not break when upgrading to future versions.

- The queries are not as complex and are easier to write.

  The views do some of the work for you. Your custom queries will not need to reference as many Protect database tables. The views join multiple tables to gather relevant information and they pull different columns from multiple tables.

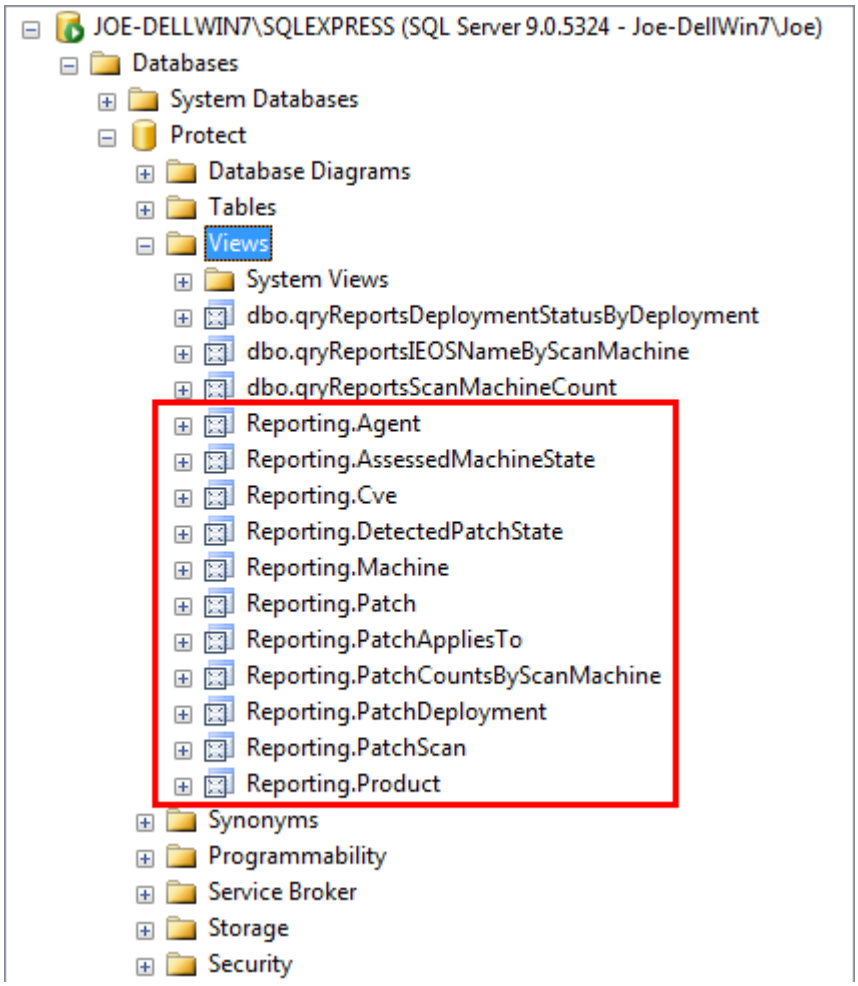
- Shavlik will continue to build out the Protect views in future versions, providing greater capabilities.
- Custom queries can be shared by trusted members of the Shavlik community.

The process for creating a custom report is as follows:

1. Familiarize yourself with the SQL Server database views that are provided with Shavlik Protect.
2. Write a database query that references the Shavlik Protect views and that generates the information you want.
3. Export the query results into the user-friendly format of your choosing.

SHAVLIK PROTECT DATABASE VIEWS

This section describes the Shavlik Protect views that can be used within a custom query. Each view provides information about the current known state of machines, focusing on patch assessments. The name of each Protect view begins with the term **Reporting**.

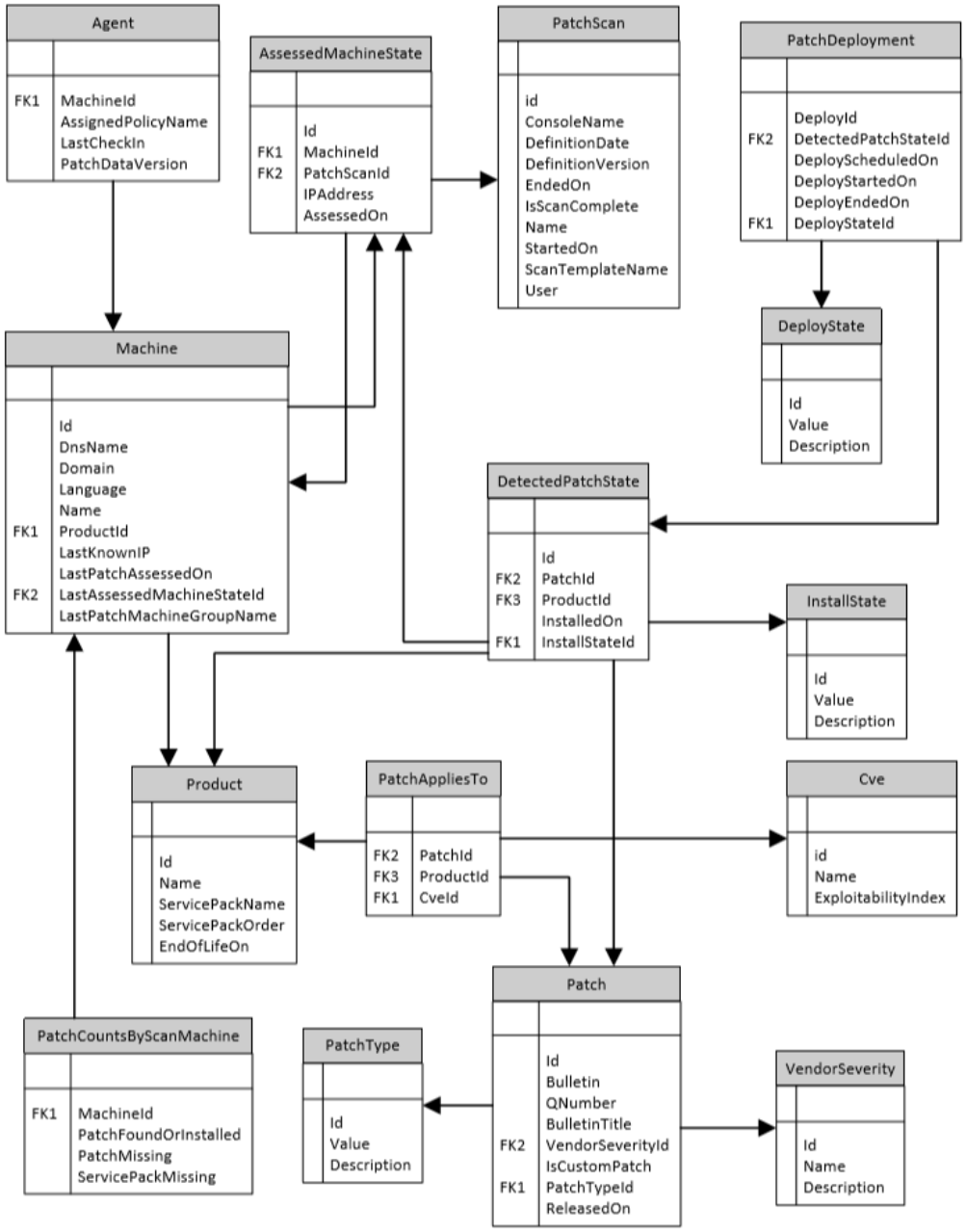


In addition, the views have relationships with the following Protect tables:

- Reporting.DeployState
- Reporting.InstallState
- Reporting.PatchType
- Reporting.VendorSeverity

Entity Relationships

This graphic shows the relationships between the Protect views (described in the remainder of this section) and the tables in the Protect database.



Agent View

The **Reporting.Agent** view displays currently known information about an installed agent.

Column Name	Data Type	Nullable	Description
MachineId	int		The machine id where the agent is installed. See [Reporting].[Machine])
AssignedPolicyName	nvarchar(256)	X	The assigned policy name.
LastCheckIn	datetime	X	The time the agent last checked in.
PatchDataVersion	nvarchar(23)	X	The patch data version used for agent assessments.

Assessed MachineState View

The **Reporting.AssessedMachineState** view displays all assessments performed on a machine.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
MachineId	int	X	The machine id of this assessment. (See [Reporting].[Machine])
PatchScanId	int	X	The patch scan id of this assessment. (See [Reporting].[PatchScan])
IPAddress	nvarchar(45)	X	The IP address of this machine. This will be displayed in IPV4 or IPV6 format.
AssessedOn	datetime	X	The assessment date.

CVE View

The **Reporting.CVE** view (Common Vulnerabilities and Exposures) displays the common vulnerability and exposure name and the exploitability index of a patch as it applies to a product.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
Name	nvarchar(13)		The name of the CVE.
ExploitabilityIndex	int		The exploitability index.

DeployState View

The **Reporting.DeployState** view defines deployment states.

Column Name	Data Type	Nullable	Description
Id	int		The deploy state id
Value	nvarchar(100)		The value of the deploy state
Description	nvarchar(512)		A description of the deploy state

Content

Run the following query to generate the contents for the **Reporting.DeployState** view.

```
SELECT [Id]
      ,[Value]
      ,[Description]
  FROM [Protect].[Reporting].[DeployState]
```

DetectedPatch State View

The **Reporting.DetectedPatchState** view displays the state of a patch found on a machine.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
AssessedMachineStateId	int		The assessed machine state id. See [Reporting].[AssessedMachineState])
PatchId	int		The patch id. See [Reporting].[Patch])
ProductId	int		The product id. See [Reporting].[Product])
InstalledOn	datetime	X	The date the patch was installed.
InstallStateId	int	X	The install state Id. (See [Reporting].[InstallState])

InstallState View

The **Reporting.InstallState** view defines installation states.

Column Name	Data Type	Nullable	Description
Id	int		The install state id.
Value	nvarchar(100)		The string value of the Id
Description	nvarchar(256)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the **Reporting.InstallState** view.

```
SELECT [Id]
      ,[Value]
      ,[Description]
  FROM [Protect].[Reporting].[InstallState]
```

ID	Value	Description
-1	Not Recorded	A service pack level detection error has occurred or the product level is an unsupported version.
0	Warning	Indicates a problem with the patch and rarely, if ever, occurs. This value can, however, occur in old patch data.
1	Note	A note exists for this patch. Please reference the QNumber on vendor web sites for more information.
2	Informational	No patches were detected for this product. Either all patches were applied or no patches exist.
3	Installed	A patch is installed.
4	Missing Patch	A missing patch was detected.
5	Missing Service Pack	A missing service pack was detected.

Machine View

The **Reporting.Machine** view displays currently known information about a machine that has been assessed.

Column Name	Data Type	Nullable	Description
Id	int		The unique identifier.
DnsName	nvarchar(255)	X	The dns name of this machine.
Domain	nvarchar(255)	X	The domain name of this machine.
Language	Int	X	The language used on this machine.
Name	nvarchar(255)	X	The netbios name of this machine.
ProductId	int	X	The product id. See [Reporting].[Product])
LastKnownIP	nvarchar(45)	X	The IP address of this machine. This will be displayed in IPV4 or IPV6 format.
LastPatchAssessedOn	datetime	X	The time this machine was last assessed upon. (This is the date the machine was scanned, not the date of the patch scan scheduled).
LastAssessedMachineStateId	Int	x	The id of the last assessed machine state.
LastPatchMachineGroupName	Nvarchar(*)	X	The name of the machine group where this machine was defined.

Patch View

The **Reporting.Patch** view displays patch information

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Bulletin	nvarchar(255)		The patch bulletin.
QNumber	nvarchar(255)		The QNumber.
BulletinTitle	nvarchar(255)	X	The patch bulletin title.
VendorSeverityId	Int	X	The vendor severity. (See [Reporting].[VendorSeverity])
IsCustomPatch	bit		Indicates if this is a custom patch.
PatchTypeId	Int	X	The patch type id. (See [Reporting].[PatchType])
ReleaseOn	datetime	X	The date this patch was released.

PatchApplies To View

The **Reporting.PatchAppliesTo** view identifies the products and CVEs that a patch applies to.

Column Name	Data Type	Nullable	Description
PatchId	int		The patch id.
ProductId	int		The product id. See [Reporting].[Product])
CveId	int	X	The cve id. See [Reporting].[Cve)

Patch Deployment View

The **Reporting.PatchDeployment** view displays patch deployment information.

Column Name	Data Type	Nullable	Description
DeployId	int		Identifies the deployment associated with this patch.
DetectedPatchStateId	int		The detected patch state id.
DeployScheduledOn	datetime	X	The date the patch was scheduled for deployment (local time).
DeployStartedOn	Datetime	X	The date the patch installation started (GMT).
DeployEndOn	Datetime	X	The date the patch installation ended (GMT).
DeployStateId	int	X	The deployment status Id. (See [Reporting].[DeployState])

Content

You can run the following query to display **DisplayStateID** values and descriptions.

```
SELECT [Id]
      ,[Value]
      ,[Description]
FROM [Protect].[Reporting].[DeployState]
```

PatchScan View

The **Reporting.PatchScan** view displays assessment information.

Column Name	Data Type	Nullable	Description	
Id	int		The unique identifier.	
ConsoleName	nvarchar(255)		The console name where this patch was performed.	
DefinitionDate	datetime	X	The assessment data definition.	
DefinitionVersion	nvarchar(50)	X	The assessment data definition version.	
EndedOn	datetime		The date the assessment ended.	
IsScanComlete	int		Determines if the scan is complete.	
			Value	**Description**
			0	The scan is not complete.
			1	The scan is complete.

Name	nvarchar(255)	X	The scan name.
StartedOn	datetime	X	The date the scan started.
ScanTemplateName	nvarchar(255)	X	The scan template name.
User	nvarchar(4000)	X	The name of the user that performed the scan.

PatchType View

The **Reporting.PatchType** view defines patch types.

Column Name	Data Type	Nullable	Description
Id	int		The patch type id.
Value	nvarchar(100)		The string value of the Id
Description	nvarchar(256)	X	Provides a simple description of the value.

Content

You can run the following query to verify the contents of the **Reporting.PatchType** view.

```
SELECT [Id]
      ,[Value]
      ,[Description]
 FROM [Protect].[Reporting].[PatchType]
```

ID	Value	Description
0	Security Patches	Microsoft Security Patches
1	Security Patches	
2	Software Distribution	
3	Security Tools	
4	Non-security Patches	
6	Custom Actions	

Product View

The **Reporting.Product** view identifies unique product and service pack combinations.

Column Name	Data Type	Nullable	Description
Id	int		This is the unique identifier.
Name	nvarchar(255)		The product name.
ServicePackName	nvarchar(50)		The service pack name.
ServicePackOrder	int	X	The service pack order.
EndOfLifeOn	datetime	X	The end of life date of this product.

Vendor Severity View

The **Reporting.VendorSeverity** view defines vendor severity states.

Column Name	Data Type	Nullable	Description
Id	int		The vendor severity id.
Name	nvarchar(100)		The name of the vendor severity.
Description	nvarchar(256)		The vendor severity description.

Content

You can run the following query to verify the contents of the **Reporting.VendorSeverity** view.

```
SELECT [Id]
      ,[Value]
      ,[Description]
  FROM [Protect].[Reporting].[VendorSeverity]
```

ID	Value	Description
0	None	None
1	Critical	A vulnerability whose exploitation could allow the propagation of an Internet worm without user action.
2	Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users'' data, or of the integrity or availability of processing resources.
3	Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation.
4	Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

SAMPLE QUERIES

The Protect views provide access to data that is in the Shavlik Protect database but that is not available in the predefined reports. This section provides sample queries that illustrate how to reference a Protect view.

Sample Query: CVE Vulnerability Report

```
/*
 This is a CVE vulnerability report that will display the CVE name and
how many machines are affected due to a missing patch on the latest patch
scan.
 */

SELECT
    cve.[Name] AS [CVE Name],
    cve.[Id] AS [CVE ID],
    patch.[Bulletin] AS [Bulletin Id],
    patch.[QNumber] AS QNumber,
    COUNT( DISTINCT machine.[Id]) AS [Machines Missing Count]
FROM
    [Reporting].[Machine] AS machine
INNER JOIN
    [Reporting].[AssessedMachineState] AS latestAssessedMachineState ON
        latestAssessedMachineState.[machineId] = machine.[Id] AND
        latestAssessedMachineState.[Id] =
machine.[LastAssessedMachineStateId]
INNER JOIN
    [Reporting].[DetectedPatchState] AS detectedPatchState ON
        detectedPatchState.[AssessedMachineStateId] =
latestAssessedMachineState.[Id]
INNER JOIN
    [Reporting].[InstallState] AS installState ON
        installState.[Id] = detectedPatchState.[InstallStateId]
INNER JOIN
    [Reporting].[Patch] AS patch ON
        patch.[Id] = detectedPatchState.[PatchId]
INNER JOIN
    [Reporting].[PatchAppliesTo] AS patchAppliesTo ON
        patchAppliesTo.[PatchId] = patch.[Id]
INNER JOIN
    [Reporting].[Cve] AS cve ON
        cve.[Id] = patchAppliesTo.[CveId]
WHERE
    /* Id 4 indicates a missing patch */
    installState.[Id] = 4
GROUP BY
    cve.[Name],
    cve.[Id],
    patch.[Bulletin],
    patch.[QNumber];
```

Sample Query: Patch Status Detail

```
/*
   This query example gets a list of installed and missing patches from
the latest scan for each machine.
*/
SELECT DISTINCT
    patch.[QNumber] AS [QNumber],
    patch.[Bulletin] AS [Bulletin Id],
    patch.[ReleasedOn] AS [Released On],
    product.[Name] AS [Product Name],
    product.[ServicePackName] AS [Service Pack Name],
    installState.[Value] AS [Install state],
    patchScan.[StartedOn] AS [ScanDate],
    machine.[Name] AS [Machine Name],
    machine.[Domain] AS Domain,
    locale.[name] AS [Language Name],
    machine.[LastKnownIP] AS [IP Address],
    machine.[LastPatchAssessedOn] AS [Scan Date],
    detectedPatchState.[InstalledOn] AS [Installed On]
FROM
    [Reporting].[PatchScan] AS patchScan
INNER JOIN
    [Reporting].[AssessedMachineState] AS assessedMachineState ON
        assessedMachineState.[PatchScanId] = patchScan.[Id]
INNER JOIN
    [Reporting].[Machine] AS machine ON
        machine.[LastAssessedMachineStateId] = assessedMachineState.[id]
INNER JOIN
    [Reporting].[DetectedPatchState] AS detectedPatchState ON
        detectedPatchState.[AssessedMachineStateId] =
assessedMachineState.[Id]
INNER JOIN
    [Reporting].[Patch] AS patch ON
        detectedPatchState.[PatchId] = patch.[Id]
INNER JOIN
    [Reporting].[InstallState] AS installState ON
        installState.[Id] = detectedPatchState.[InstallStateId]
INNER JOIN
    [Reporting].[Product] AS product ON
        product.[Id] = detectedPatchState.[ProductId]
LEFT OUTER JOIN
    [sys].[syslanguages] AS locale ON
        machine.[Language] = locale.[lcid] /* machine.[Language] is used
to index into [sys].[syslanguages] */
WHERE
    (
        detectedPatchState.[InstallStateId] = 3 OR  /* Installed Patch */
        detectedPatchState.[InstallStateId] = 4     /* Missing Patch */
     )
ORDER BY
     patch.[Bulletin],
    patch.[QNumber],
    machine.[Name]
```

Sample Query: Missing Patches by Agent Policy

```
/*
 * Select all missing patches for the last scan of machines associated to
an agent policy.
 * The following data is displayed
 *   Assigned Policy Name
 *   Machine Name
 *   Bulletin Id
 *   QNumber
 *   Product Name
 *   Service Pack
 *   Patch Install State
*/
SELECT
    agent.[AssignedPolicyName] AS [Assigned Policy Name],
    machine.[Name] AS [Machine Name],
    machine.[Domain] AS Domain,
    patch.[Bulletin] AS [Bulletin Id],
    patch.[QNumber] AS QNumber,
    product.[Name] AS [Product Name],
    product.[ServicePackName] AS [Service Pack],
    installState.[Value] AS [Patch Install State],
    product.[id] AS ProductId,
    detectedPatchState.[ProductId] AS [detectedPatchState ProductID]
FROM
    [Reporting].[Agent] AS agent
INNER JOIN
    [Reporting].[Machine] AS machine ON
        machine.[Id] = agent.[MachineId]
INNER JOIN
    [Reporting].[AssessedMachineState] AS assessedMachineState ON
        assessedMachineState.[Id] = machine.[LastAssessedMachineStateId]
INNER JOIN
    [Reporting].[DetectedPatchState] AS detectedPatchState ON
        detectedPatchState.[AssessedMachineStateId] =
    assessedMachineState.[Id]
INNER JOIN
    [Reporting].[Patch] AS patch ON
        patch.[Id] = detectedPatchState.[PatchId]
INNER JOIN
    [Reporting].[Product] AS product ON
        product.[Id] = detectedPatchState.[ProductId]
INNER JOIN
    [Reporting].[InstallState] AS installState ON
        installState.[Id] = detectedPatchState.[InstallStateId]
WHERE
    /* Id 4 indicates a missing patch */
    installState.[Id] = 4
ORDER BY
    agent.[AssignedPolicyName],
    machine.[Name],
    machine.[Domain],
    patch.[Bulletin]
```