Application Note: Veritas High Availability solution for DLP Enforce Server

Windows

December 2011

Application Note: Veritas High Availability solution for DLP Enforce Server

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043
www.symantec.com

Third-party legal notices

Third-party software may be recommended, distributed, embedded, or bundled with this Symantec product. Such third-party software is licensed separately by its copyright holder.

Technical support

Visit http://www.symantec.com/business/support/assistance_care.jsp for product assistance. Use the Knowledge Base search feature to access resources such as TechNotes, product alerts, software downloads, hardware compatibility lists, and our customer email notification service. If you encounter an error when using a product, include the error number preceding the message when contacting Technical Services. You can also use the error number to search for information in TechNotes or documents on the Web site.

Veritas High Availability solution for DLP Enforce Server

Introduction

This application note describes the Veritas High Availability Solution for Data Loss Prevention (DLP) Enforce Server.

In this solution, DLP Enforce Server services are managed using the GenericService agent. The GenericService agent brings specific Enforce Server services online, monitors their state, detects failures, and takes the services offline.

About Data Loss Prevention

Data Loss Prevention (DLP) answers three fundamental questions:

- Where is your confidential data?
- How is it being used?
- How do you prevent data loss?

Symantec DLP delivers a unified solution to discover, monitor, and protect confidential data wherever it is stored or used.

Symantec DLP Enforce Platform automatically enforces universal Data Loss Prevention policies with a centralized platform for detection, incident remediation workflow and automation, reporting, system management and security.

For additional information refer to the DLP documentation.

Supported software

The Veritas High Availability solution for DLP Enforce Server supports the following software:

Veritas Cluster Server (VCS)	VCS 5.1 Service Pack 2 or later
Operating Systems	Microsoft Windows Server 2008 R2 (x64) or later
Data Loss Prevention (DLP)	11.1
Component	Enforce Server

About DLP Enforce Server

DLP installation tiers

Symantec Data Loss Prevention supports three different installation types:

- Single-tier
  To implement the single-tier installation, you install the database, the Enforce Server, and a detection server, all on the same computer.
- Two-tier
  To implement the two-tier installation, you install the Oracle database and the Enforce Server on the same computer. You then install detection servers on separate computers.
- Three-tier
  To implement the three-tier installation, you install the Oracle database, the Enforce Server, and a detection server on separate computers. Symantec recommends implementing the three-tier installation architecture as it enables your database administration team to control the database. In this way you can use all of your corporate standard tools for database backup, recovery, monitoring, performance, and maintenance. Three-tier installations require that you install the Oracle Client (SQL*Plus and Database Utilities) on the Enforce Server to communicate with the Oracle server.

This solution also provides details on the required VCS configuration based on the type of installation tier.

DLP Enforce Server services

The Symantec Data Loss Prevention services for the Enforce Server are described in Table 2-1.

Table 2-1 Services on the Enforce Server

Service	Description
Vontu Manager	Provides the centralized reporting and management services for Symantec Data Loss Prevention.
Vontu Monitor Controller	Controls the detection servers (monitors).
Vontu Notifier	Provides the database notifications.
Vontu Incident Persister	Writes the incidents to the database.

Table 2-1 Services on the Enforce Server

Service	Description
Vontu Update	Installs the Symantec Data Loss Prevention system updates. This service only runs during system updates and upgrades.

Components of the High Availability solution for DLP Enforce Server

Veritas Storage Foundation and High Availability Solutions for DLP Enforce Server on Windows contains the following components:

Storage Foundation for Windows

Veritas Storage Foundation for Windows (SFW) brings advanced volume management technology, quick recovery, and fault tolerant capabilities to enterprise computing environments.

Veritas Cluster Server

Veritas Cluster Server (VCS) provides is a high availability solution that monitors system and application services and restarts services when hardware or software fails.

A VCS cluster connects multiple independent systems to provide failover capability thus reducing application downtime. VCS supports local, metropolitan, and global clusters.

VCS Oracle agent on Windows

DLP Enforce Server stores incident data in Oracle database. The VCS database agent for Oracle provides high availability for Oracle in a VCS cluster. The VCS database agent for Oracle monitors the Oracle database and listener services, brings them online, and takes them offline. Refer to *Veritas Cluster Server Database Agent for Oracle Configuration Guide* for additional information.

VCS GenericService agent on Windows used to cluster DLP Enforce services

The GenericService agent brings services online, takes them offline, and monitors their status. Note that a service is an application type supported by Windows that conforms to the interface rules of the Service Control Manager (SCM).

Agent functions

Table 2-2 describes the agent functions.

Table 2-2 Agent functions

online	Starts the configured service.
offline	Stops the configured service.
monitor	Retrieves the current state of the configured service. It also verifies the user context, if applicable.

Note: The service to be configured using the GenericService agent must have the status as Stopped and the startup type as Manual.

Symantec Data Loss Prevention includes the following services which can be clustered using the GenericService agent:

- Vontu Manager
- Vontu Incident Persister
- Vontu Notifier
- Vontu Update
- Vontu Monitor Controller

Note: On Windows platforms, all DLP services run under the System Account user name (by default, protect), except for the Vontu Update services, which is run under *username*_update (by default, protect_update).

For additional information on the GenericService agent, refer to *Veritas Cluster Server Bundled Agents Reference Guide for Windows*.

VCS Storage agents on Windows

Storage agents make your shared storage highly available. Volume Manager Diskgroup (VMDg) and MountV agents provide high availability for shared disks and volumes managed using Storage Foundation for Windows.

For additional information on the storage agents, refer to *Veritas Cluster Server Bundled Agents Reference Guide on Windows*.

VCS Network agents on Windows

Network agents make IP addresses and computer names highly available. The NIC and IP agents work together to make a virtual IP address highly available. The Lanman agent makes a virtual computer name highly available. The Lanman agent requires the IP agent for operation.

For additional information on the network agents, refer to *Veritas Cluster Server Bundled Agents Reference Guide on Windows*.

Installing and configuring DLP Enforce Server for high availability

This section includes the installation and configuration requirements for the various components that are involved in making the DLP Enforce Server highly available. References are provided to product documentation based on the involved component of the solution.

Installation of SFWHA

You should install the Veritas Storage Foundation High Availability for Windows (SFWHA), on all the systems that will host the DLP Enforce Server or Oracle database.

The *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide* provides information on how to install or upgrade SFWHA for Windows. Information related to services and ports used by SFWHA is also provided.

Administration of VCS service groups

The *Veritas Cluster Server Administrator's Guide* explains clustering concepts and terminology. It provides information on how to administer VCS resources and service groups using the Java console as well as using the command line. Troubleshooting information is also included.

Setting up Oracle for High Availability

Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide provides Oracle installation or upgrade steps. It also provides the steps to create the Symantec Data Loss Prevention database and the required Oracle accounts.

- For single-tier and two-tier Symantec Data Loss Prevention installations, Oracle is installed on the Enforce Server.

- For a three-tier installation, Oracle is installed on a separate server. For a three-tier installation, the Oracle Client (SQL*Plus and Database Utilities) must be installed on the Enforce Server computer to enable communication with the Oracle server.

The strategy for installing Oracle in a VCS cluster is aimed at ensuring that Oracle installation on all the nodes in the cluster is uniform. This involves installing the Oracle binaries locally on each system. You can perform this installation simultaneously on cluster nodes. The installer screens and options may vary slightly for different versions of Oracle. *Veritas Cluster Server Database Agent for Oracle Configuration Guide* lists the VCS requirements for Oracle installation and how to configure corresponding VCS resources for this Oracle installation.

By switching the Oracle service group between VCS cluster nodes you can verify that Oracle is correctly setup for high availability.

Setting up DLP Enforce Server for High Availability

- Before installing DLP Enforce Server, ensure that the Oracle software and Symantec Data Loss Prevention database are installed on the cluster nodes that can host the Oracle database.
- DLP Enforce Server should be installed on all cluster nodes so that services for DLP Enforce Server get created on all possible failover nodes.
- Virtualization of storage components
  The Symantec DLP installation directory should be present on the shared storage. VCS storage agents make the shared storage highly available.
  The default installation directory is: `c:\Vontu.`
  Symantec recommends that you use the default installation directory.
- Ensure that the 'protect' user has the correct permissions to access and modify contents of the DLP installation directory on all the cluster nodes.
- The jdbc.properties file must be updated with the Oracle virtual IP information to ensure that Oracle failover works correctly.
  VCS Network agents make IP addresses and computer names highly available.

Configuring the VCS service groups for DLP Enforce Server

The high availability solution for DLP Enforce Server involves creating the following service groups:

- DLP Enforce service group - for clustering the DLP Enforce services

In the DLP Enforce service group, each DLP Enforce service is clustered using a resource of type GenericService. Before starting other DLP services, the Vontu Notifier service must be started. This requirement is captured by having VCS resources corresponding to other DLP services depend on the VCS resource for Vontu Notifier service. Also, VCS resources are created for storage and network components required by DLP.

- Oracle service group - for clustering the Oracle database and listener
  In Oracle service group, Oracle database and listener are clustered using Oracle and Netlistener resources. Also, VCS resources are created for storage and network components required by Oracle.

Effect of DLP installation tiers on the VCS service group configuration

Symantec recommends that Oracle resources and Enforce Server resources should be part of different service groups.

- For Single-tier and Two-tier DLP installations: Symantec recommends that the DLP Enforce service group should have the *Online Local Firm dependency* on Oracle service group. This service group level dependency will ensure that both the service groups are online on the same node in the cluster.
- For Three-Tier installations: Symantec recommends that DLP Enforce service group should have the *Online Global Firm dependency* on Oracle service group. With this configuration, the Oracle service group can be brought online on any node of the cluster and DLP Enforce service group can be brought online independently on any other node in the cluster.

For additional information about the service group dependencies refer to *Veritas Cluster Server Administrator's Guide*.

Sample configurations

The sample configurations graphically depict the resource types, resources, and resource dependencies within the service group. Review these dependencies carefully before configuring the DLP Enforce services using the GenericService agent.

For more information about these resource types, see the *Veritas Cluster Server Bundled Agents Reference Guide on Windows*.

Sample GenericService agent resource type definition

```
type GenericService (
      static i18nstr ArgList[] = { ServiceName,
DelayAfterOnline, DelayAfterOffline, UserAccount,
Password, Domain, service_arg, UseVirtualName,
"LanmanResName:VirtualName" }
      i18nstr ServiceName
      int DelayAfterOnline = 10
      int DelayAfterOffline = 10
      i18nstr UserAccount
      str Password
      i18nstr Domain
      str service_arg[]
      boolean UseVirtualName = 0
      str LanmanResName
)
```

Sample configuration in a VCS environment

This sample main.cf file includes GenericService agent resources used to cluster the DLP Enforce services and Oracle agent resource to cluster the Oracle database.

This sample configuration is for a three-tier installation of DLP. The service group level dependency must be changed based on the DLP installation tiers.

```
include "types.cf"
cluster DLPClus (
   UserNames = { admin = GnoGniNkoJooMwoInl, a = dqqK }
   Administrators = { admin, a }
   )

system NODE1 (
   )

system NODE2 (
   )
```

```
group DLPSG (
    SystemList = { NODE1 = 0, NODE2 = 1 }
    )

    GenericService VontuNotifier_res (
        ServiceName = VontuNotifier
        )

    GenericService VontuIncidentPersister_res (
        ServiceName = VontuIncidentPersister
        )

    GenericService VontuMonitorController_res (
        ServiceName = VontuMonitorController
        )

    GenericService VontuUpdate_res (
        ServiceName = VontuUpdate
        )

    GenericService VontuManager_res (
        ServiceName = VontuManager
        )

    IP dlp_ip_res (
        Address = "10.209.68.246"
        SubNetMask = "255.255.252.0"
        MACAddress @NODE1 = 00-1D-09-65-E9-3B
        MACAddress @NODE2 = 00-1D-09-65-D5-8C
        )

    Lanman EnforceHost_lanman_res (
        VirtualName = enforcehost
        IPResName = dlp_ip_res
        )

    MountV dlp_mount_res (
        MountPath = "C:\\Vontu"
        VolumeName = DlpSofvol
        VMDGResName = dlp_dg_res
        )

    NIC dlp_nic_res (
        Enabled = 0
        MACAddress @NODE1 = 00-1D-09-65-E9-3B
        MACAddress @NODE2 = 00-1D-09-65-D5-8C
        )

    VMDg dlp_dg_res (
        DiskGroupName = DlpSofdg
        )
```

```
requires group OraSG online global firm
VontuNotifier_res requires dlp_mount_res
VontuNotifier_res requires EnforceHost_lanman_res
VontuIncidentPersister_res requires VontuNotifier_res
VontuMonitorController_res requires VontuNotifier_res
VontuUpdate_res requires dlp_mount_res
VontuManager_res requires VontuNotifier_res
dlp_ip_res requires dlp_nic_res
EnforceHost_lanman_res requires dlp_ip_res
dlp_mount_res requires dlp_dg_res

// resource dependency tree
//
// group DLPSG
// {
// GenericService VontuIncidentPersister_res
//     {
//     GenericService VontuNotifier_res
//         {
//         MountV dlp_mount_res
//             {
//             VMDg dlp_dg_res
//             }
//         Lanman EnforceHost_lanman_res
//             {
//             IP dlp_ip_res
//                 {
//                 NIC dlp_nic_res
//                 }
//             }
//         }
//     }
// GenericService VontuMonitorController_res
//     {
//     GenericService VontuNotifier_res
//         {
//         MountV dlp_mount_res
//             {
//             VMDg dlp_dg_res
//             }
//         Lanman EnforceHost_lanman_res
//             {
//             IP dlp_ip_res
//                 {
//                 NIC dlp_nic_res
//                 }
//             }
//         }
//     }
// GenericService VontuUpdate_res
//     {
//     MountV dlp_mount_res
```

```
    //          {
    //          VMDg dlp_dg_res
    //          }
    //      }
    // GenericService VontuManager_res
    //      {
    //      GenericService VontuNotifier_res
    //          {
    //          MountV dlp_mount_res
    //              {
    //              VMDg dlp_dg_res
    //              }
    //          Lanman EnforceHost_lanman_res
    //              {
    //              IP dlp_ip_res
    //                  {
    //                  NIC dlp_nic_res
    //                  }
    //              }
    //          }
    //      }
    // }

group OraSG (
    SystemList = { NODE1 = 0, NODE2 = 1 }
    )

    IP ora_ip_res (
        Address = "10.209.68.244"
        SubNetMask = "255.255.252.0"
        MACAddress @NODE1 = 00-1D-09-65-E9-3B
        MACAddress @NODE2 = 00-1D-09-65-D5-8C
        )

    MountV ora_mount_res (
        MountPath = "C:\\oracle\\db"
        VolumeName = DbVol
        VMDGResName = ora_dg_res
        )

    NIC ora_nic_res (
        MACAddress @NODE1 = 00-1D-09-65-E9-3B
        MACAddress @NODE2 = 00-1D-09-65-D5-8C
        )

    Netlsnr netlsnr_res (
        ServiceName = OracleOraDb11g_home1TNSListener
        )

    Oracle oradb_protect_res (
        ServiceName = OracleServicePROTECT
        Domain = isv
```

```
        SID = protect
        UserName = administrator
        EncryptedPasswd = JXPvMXm
        SQLFile = "C:\\Program Files\\Veritas\\cluster
server\\bin\\Oracle\\check.SQL"
        )

    VMDg ora_dg_res (
        DiskGroupName = DlpDBdg
        )

    netlsnr_res requires oradb_protect_res
    oradb_protect_res requires ora_mount_res
    oradb_protect_res requires ora_ip_res
    ora_mount_res requires ora_dg_res
    ora_ip_res requires ora_nic_res

    // resource dependency tree
    //
    // group OraSG
    // {
    // Netlsnr netlsnr_res
    //     {
    //     Oracle oradb_protect_res
    //         {
    //         MountV ora_mount_res
    //             {
    //             VMDg ora_dg_res
    //             }
    //         IP ora_ip_res
    //             {
    //             NIC ora_nic_res
    //             }
    //         }
    //     }
    // }
```

Group dependencies

Service group dependency (Java console view)

The following figures illustrate a sample VCS configuration with different service group dependencies, based on the DLP installation tiers.

Figure 2-1 Service group dependency view for a 3-tier installation of DLP

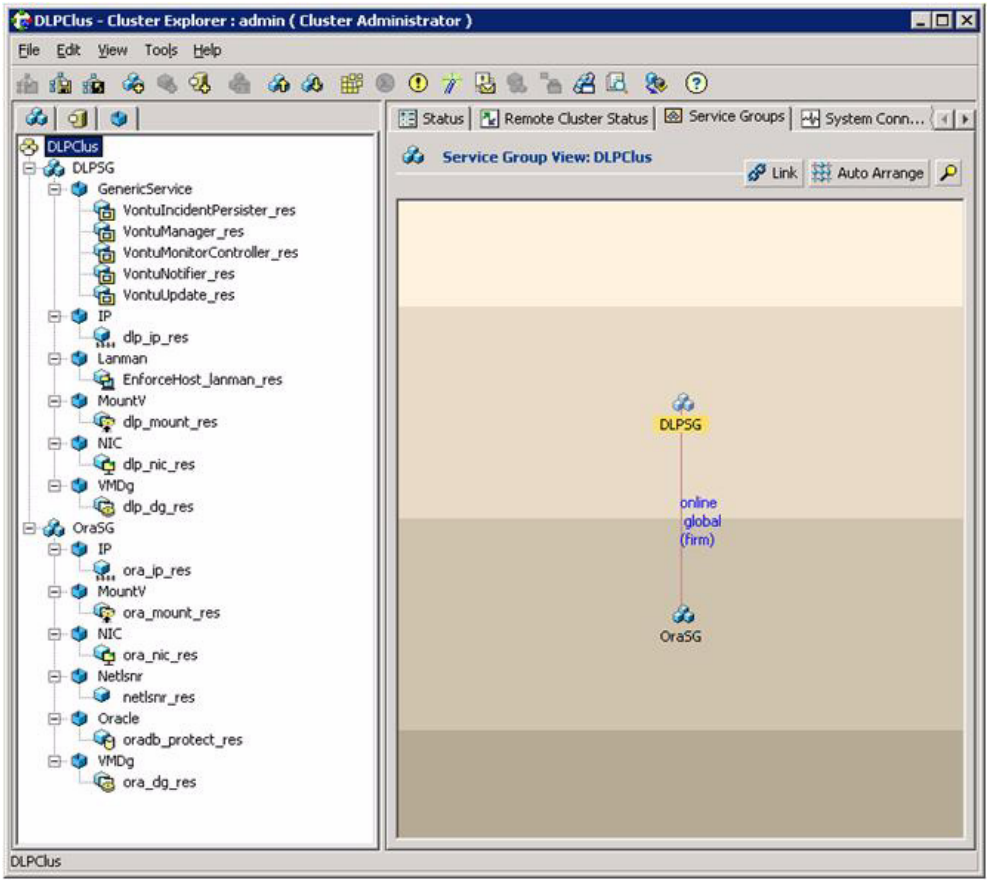


Figure 2-1 shows the service group dependency graph for a 3-tier installation of DLP; the DLP Enforce service group has an Online Global Firm dependency on the Oracle service group.

Figure 2-2 Service group dependency view for a 2-tier installation of DLP

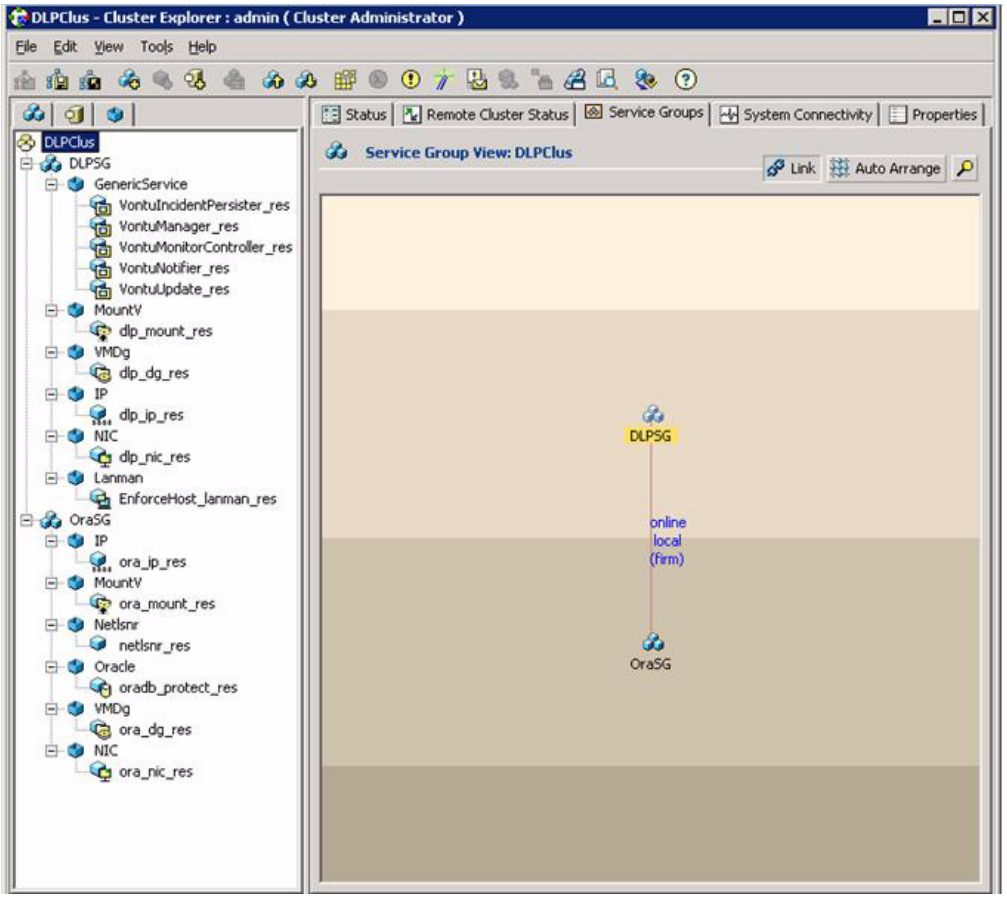


Figure 2-2 shows a service group dependency graph for a 2-tier installation of DLP; the DLP Enforce service group has an Online Local Firm dependency on the Oracle service group.

Resource dependency (Java console view)

The following figures illustrate a sample VCS configuration with different resource dependencies for the DLP Enforce service group and the Oracle service group.

Figure 2-3 Resource dependency view for the DLP Enforce service group

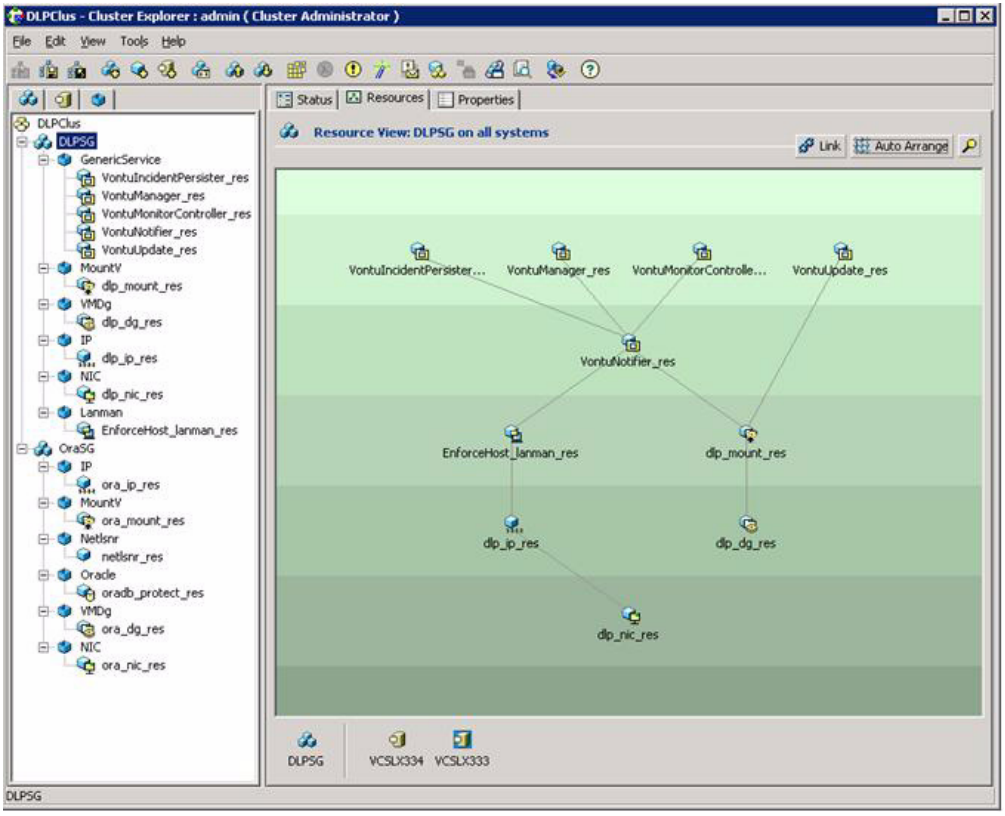


Figure 2-3 shows a resource dependency graph for the DLP Enforce Server service group. In this graph, the resources corresponding to the Vontu Incident Persister service, Vontu Manager service, and Vontu Monitor Controller service depend on the resource for the Vontu Notifier service. The storage and network resources provide the necessary infrastructure for the Vontu services.

Figure 2-4 Resource dependency view for the Oracle service group

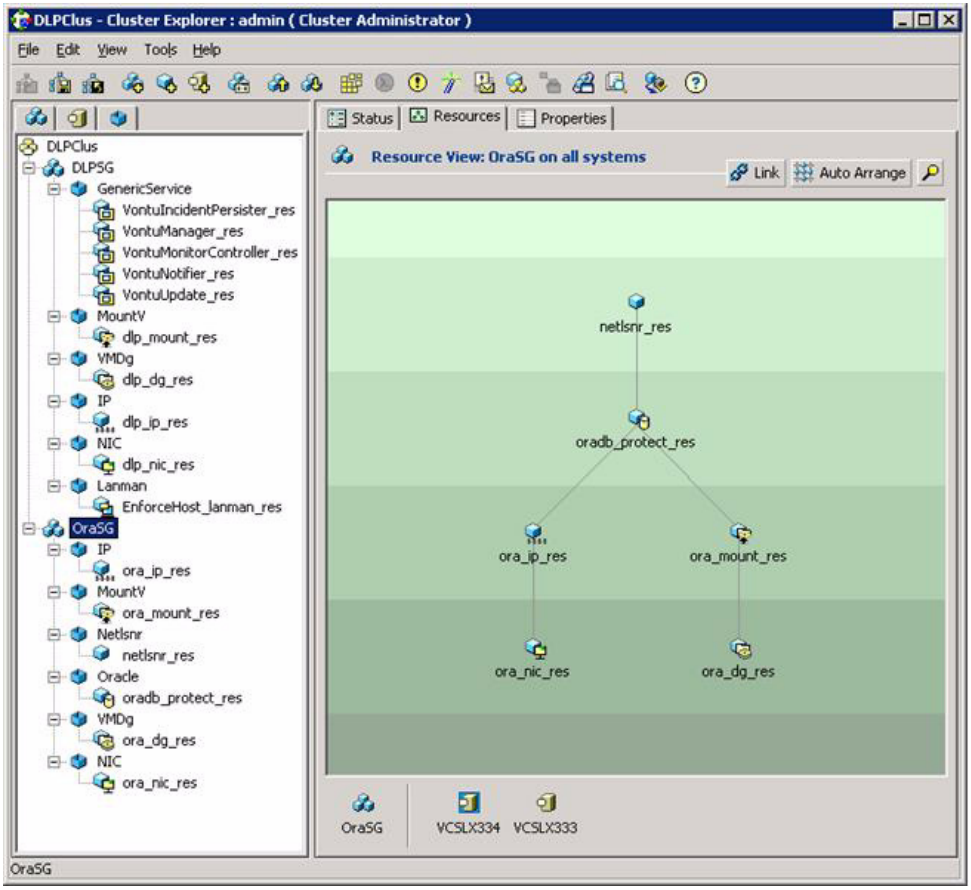
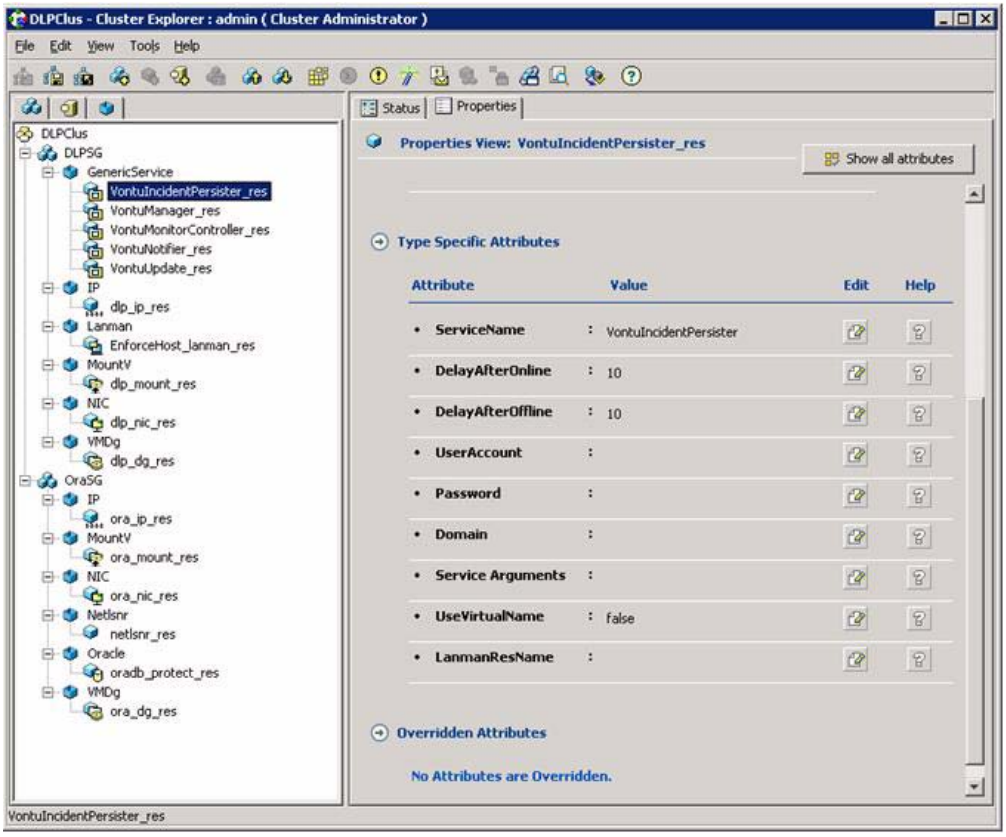


Figure 2-4 shows a resource dependency view for the Oracle service group. In this resource dependency graph for the Oracle service group, the Netlsnr resource depends on the Oracle resource, which in-turn depends on the storage and network resources.

Properties for GenericService resource (Java console view)

The following figures illustrate a sample VCS configuration with properties set for the GenericService resource corresponding to the Vontu Incident Persister service. The properties for the other Vontu services must be set in a similar manner.

Figure 2-5 Properties view for GenericService resource corresponding to Vontu Incident Persister service



In Figure 2-5, for the above GenericService resource corresponding to Vontu Incident Persister service, the ServiceName attribute is set to VontuIncidentPersister.

Troubleshooting

This section describes how to troubleshoot common problems in VCS GenericService, Oracle agents and DLP. References are provided to appropriate product documentation.

VCS GenericService agent and other VCS bundled agents

VCS Logging

VCS generates two error message logs: the engine log and the agent log. Log file names are appended by letters. The letter A indicates the first log file, B the second, C the third, and so on.

The engine log is located at `%VCS_HOME%\log\engine_A.txt`.

The agent log is located at `%VCS_HOME%\log\agent_A.txt`.

GenericService agent error messages

Refer to the 'Troubleshooting services and application agents' section from the *VCS Bundled Agent Reference Guide on Windows*. This section provides a list of GenericService agent error message descriptions and recommended actions.

VCS Oracle agent troubleshooting

Refer to the 'Troubleshooting VCS agents' section from the *Veritas Cluster Server Database Agent for Oracle Configuration Guide on Windows*. This section provides a list of some commonly-encountered problems with the Oracle agent and some possible solutions. It also lists the error messages associated with the VCS database agent for Oracle.

DLP log locations

If the Symantec DLP services do not start, check the log files for possible issues (for example, connectivity, password, or database access issues).

- The Symantec DLP installation log is `c:\Vontu\.install4j\installation.log`.
- Symantec DLP operational logs are in `c:\Vontu\Protect\logs`.

Starting an Enforce Server on Windows outside VCS control

To start the Symantec DLP services on a Windows Enforce Server:

1. On the computer that hosts the Enforce Server, navigate to **Start** > **All Programs** > **Administrative Tools** > **Services**, to open the Windows Services menu.
2. Start the Vontu Notifier service.
3. Start the remaining Symantec Data Loss Prevention services, including the following services:
   - Vontu Manager
   - Vontu Incident Persister
   - Vontu Update
   - Vontu Monitor Controller

Stopping an Enforce Server on Windows outside VCS control

To stop the Symantec Data Loss Prevention Services on a Windows Enforce Server:

1. On the computer that hosts the Enforce Server, navigate to **Start** > **All Programs** > **Administrative Tools** > **Services**, to open the Windows Services menu.
2. From the Services menu, stop all running Symantec Data Loss Prevention services, which might include the following services:
   - Vontu Update
   - Vontu Incident Persister
   - Vontu Manager
   - Vontu Monitor Controller
   - Vontu Notifier

Recursive permissions for protect user on `C:\Vontu`

Ensure that the 'protect' user has the required permissions to access and modify the contents of the DLP Enforce Server installation directory (`C:\Vontu`, by default) on all the cluster nodes.