Use BlueXP operational resiliency

BlueXP operational resiliency

NetApp
May 08, 2024

Table of Contents

Use BlueXP operational resiliency

Review and remediate security risk issues

BlueXP operational resiliency enables you to review security risks related to firmware issues and implement remediations.

Recommendations are provided at the system or node level.

After reviewing risks, you can remediate those risks in two ways:

- Have the service execute the remediation, which will fix the issue for you.
- Download an Ansible playbook, an open-source deployment system that enables you to run configuration tasks, and you perform the actions suggested in the playbook.

Using the operational resiliency service, you can accomplish these goals:

- Review security risk issues
- Remediate automatically
- Remediate using an Ansible playbook
- Determine the risk remediation status

Review security risk issues

BlueXP operational resiliency identifies security risks on your on-premises ONTAP cluster.

Reviewing the risks and executing the automated remediation involves the following processes:

- Create a Connector in BlueXP (if one does not already exist for the operational resiliency service).
- Discover the cluster (if one does not already exist for the service).
- Execute the remediation or download an Ansible playbook.
- View the remediation status.

Steps

1. From the BlueXP left navigation, select **Health** > **Operational resiliency** > **Risk Remediation**.
2. In the list of risks, sort by the Impact level column to see the highest risks first.
3. Select the risk and see additional details.
4. Select **Remediate risk**.
5. Do one of the following:
    - For each cluster, select **Remediate**.

      This action leads to remediating the issue automatically (after you select **Execute** to start the remediation). Continue with Remediate risk issues automatically.

    - To remediate the issue yourself with an Ansible playbook, select **Download**. Continue with Remediate

risk issues with an Ansible playbook.

Remediate the issue automatically

If you selected the **Remediate** option in BlueXP operational resiliency, the service can implement the remediation for you.

Steps

1. From the BlueXP left navigation, select **Health** > **Operational resiliency** > **Risk Remediation**.
2. From the Risk Remediation page, sort by the Impact level column to see the highest risks first.
3. Select the risk and select **Remediate risk**.
4. For each cluster, select **Remediate**.

   Instructions appear, depending on the issue. Some of the options on this page do not appear if a BlueXP Connector exists or a cluster is known.

   - If a Connector does not exist or is not yet enabled, the service displays the Create a Connector page, where you can create the Connector. If the Connector exists, but is not active, you must enable it in the Cloud provider service.

     Refer to the BlueXP documentation that describes how to create a Connector.

   - If a cluster does not exist, the service displays a page where you identify the cluster.

     Refer to BlueXP documentation that explains how to identify the cluster.

5. After the Connector is deployed and the cluster is discovered, review the remediation.

   If you selected the **Remediate** option to have the service implement the remediation for you, the Review and Execute Required Fix page appears.

6. Review the risk and other information.
7. Select **Execute**.

   This action deploys the Connector (if not already done), discovers the cluster, downloads the fix and automatically implements the fix on the selected cluster.

8. To view the status of the remediation fix, note the cluster name on the Remediation Status page.

Remediate risks using an Ansible playbook

You can review security risks and download an Ansible playbook that you can follow to fix the issue.

You can download an Ansible playbook, an open-source deployment system that enables you to run configuration tasks. To use Ansible, simply run the playbook file, which uses the inventory and helper files stored in the same directory.

What you'll need

The system must be able access the cluster IP over the network for executing Ansible playbooks.

Steps

1. From the BlueXP left navigation, select **Health** > **Operational resiliency** > **Risk Remediation**.
2. In the list of risks, sort by the Impact level column to see the highest risks first.
3. Select the risk and select **Remediate risk**.
4. To download an Ansible playbook that you use to remediate the issue yourself, select **Download**.

   The service installs the Ansible playbook to your local machines in a location that you choose. The playbook downloads as a zip file, which contains several YML files.

5. Locate the Ansible playbook in the download folder.
6. Run the Ansible playbook:

   ```
   $ ansible-playbook <playbook.yml>
   ```

   For instructions on how to use an Ansible playbook, refer to the Ansible documentation.

7. Follow the instructions in the playbook.

Review the remediation status

You can check on the status of a remediation at any time. You can see whether it's running, completed, or failed.

Steps

1. From the BlueXP left navigation, select **Health** > **Operational resiliency** > **Remediation status**.

   The Remediation Status page appears.

2. To see details of an issue, select the issue to expand it.