Decrypt domain traffic with a Windows domain controller

Published: 2021-09-29

The ExtraHop system can be configured to retrieve and store domain keys from a domain controller. When the system observes encrypted traffic that matches the stored keys, all of the Kerberos-encrypted traffic in the domain is decrypted for supported protocols. The system only synchronizes Kerberos and NTLM decryption keys and does not modify any other properties in the domain.

A domain controller like Active Directory is a frequent target for attackers because a successful attack campaign yields high-value assets. Critical attacks can be obscured by Kerberos or NTLM decryption, such as Golden Ticket, PrintNightmare, and Bloodhound. Decrypting this type of traffic can provide deeper insight for security detections.

The following requirements must be met for decryption:

- You must have an Active Directory domain controller (DC) that is not configured as a Read-only Domain Controller (RODC).
- Only Windows Server 2016 and Windows Server 2019 are supported.
- Only one domain controller can be configured on a sensor, which means you can decrypt the traffic from one domain per sensor.
- The ExtraHop system synchronizes keys for up to 50,000 accounts in a configured domain. If your DC has more than 50,000 accounts, some traffic will not be decrypted.
- The ExtraHop system must observe the network traffic between the DC and connected clients and servers.
- The ExtraHop system must be able to access the domain controller over the following ports: TCP 88 (Kerberos), TCP 445 (SMB), TCP 135 (RPC), and TCP ports 49152-65535 (RPC dynamic range).

Add domain controller settings to the ExtraHop system

Warning: If you enable these settings, the ExtraHop system is granted access to all of the account keys in a Windows domain. The ExtraHop system should be deployed at the same security level as the domain controller. Here are some best practices to consider:

- Strictly limit end-user access to sensors that are configured with access to the domain controller. Ideally, only permit end-user access to a connected Command appliance or Reveal(x) 360.
- Configure sensors with an identity provider that has strong authentication features such as two-factor or multi-factor authentication.
- Restrict inbound and outbound traffic to and from the sensor to the minimum necessary.
- In Active Directory, limit the Logon Workstations for the account to only communicate with the domain controller that the ExtraHop system is configured with.

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the System Configuration section, click **Capture**.
3. Click **Domain Controller**.
4. Select the **Enable connection to the domain controller** checkbox.
5. Complete the following fields:

   • **Hostname:** The fully qualified domain name of the Windows server.

- **Computer Name (sAMAccountName):** The name of the Windows server.
- **Realm Name:** The Kerberos realm name of the Windows server.
- **User Name:** The name of a user who is a member of the built-in Administrators group for the domain (not to be confused with the Domain Admins group). To prevent possible connection errors, specify a user account created after the domain controller was established.
- **Password:** The password of the privileged user.

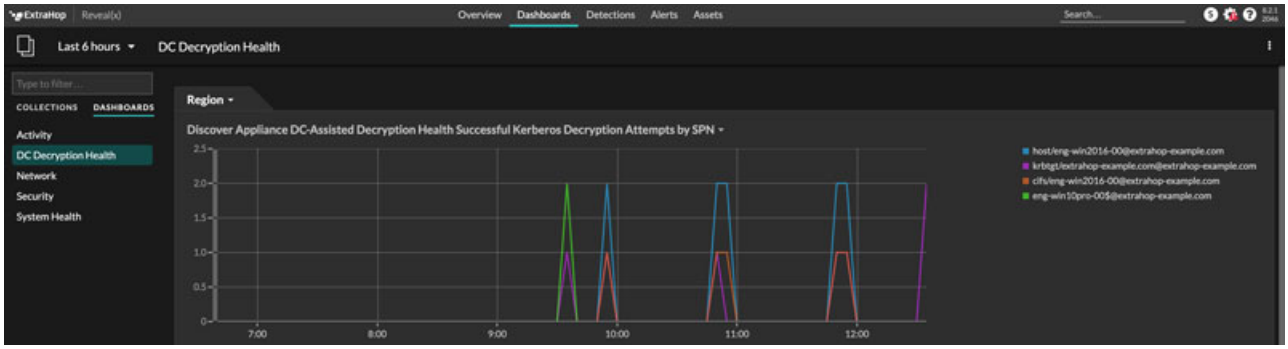
6. Click **Test Connection** to confirm that the sensor can communicate with the Windows server.
7. Click **Save**.

Validate the configuration settings

To validate that the ExtraHop system is able to decrypt traffic with the domain controller, create a dashboard that identifies successful decryption attempts.

1. Create a new dashboard.
2. Click the chart widget to add the metric source.
3. Click **Add Source**.
4. In the Sources field, type `Discover` in the search field and then select **Discover Appliance**.
5. In the Metrics field, type `DC` in the search field and then select **DC-Assisted Decryption Health - Successful Kerberos Decryption Attempts by SPN**.
6. Click **Save**.

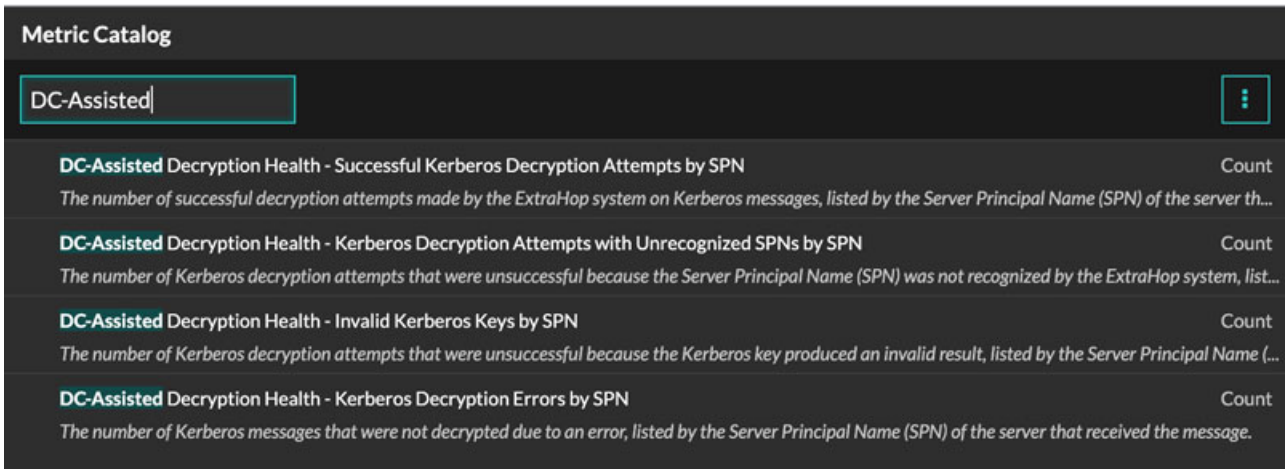
The chart appears with a count of successful decryption attempts.



Additional system health metrics

The ExtraHop system provides metrics that you can add to a dashboard to monitor DC-assisted decryption health and functionality.

To view a list of available metrics, click the System Settings icon and then click **Metric Catalog**. Type `DC-Assisted` in the filter field to display all available DC-assisted decryption metrics.


Metric Catalog
DC-Assisted
DC-Assisted Decryption Health - Successful Kerberos Decryption Attempts by SPN
Count
The number of successful decryption attempts made by the ExtraHop system on Kerberos messages, listed by the Server Principal Name (SPN) of the server th...
DC-Assisted Decryption Health - Kerberos Decryption Attempts with Unrecognized SPNs by SPN
Count
The number of Kerberos decryption attempts that were unsuccessful because the Server Principal Name (SPN) was not recognized by the ExtraHop system, list...
DC-Assisted Decryption Health - Invalid Kerberos Keys by SPN
Count
The number of Kerberos decryption attempts that were unsuccessful because the Kerberos key produced an invalid result, listed by the Server Principal Name (...
DC-Assisted Decryption Health - Kerberos Decryption Errors by SPN
Count
The number of Kerberos messages that were not decrypted due to an error, listed by the Server Principal Name (SPN) of the server that received the message.